ACCUKNOX

Zero Trust
CNAPP
Cloud Native Application Protection
Definitive Guide

Secure
Build → Runtime
Public Cloud (AWS, Azure, GCP), Private / Air gapped, Edge/IoT
Kubernetes, Virtual Machine
Static, Dynamic workloads

Table of Contents

Chapter

1. Zero Trust
2. Zero Trust CNAPP
3. About AccuKnox

CSPM

AccuKnox Cloud Security Posture Management (CSPM) leverages agentless technology to revolutionize cloud security by proactively identifying, prioritizing vulnerabilities, providing a seamless orchestration and management platform.

CWPP

Runtime Protection Reinvented: AccuKnox Cloud Workload Protection Platform (CWPP) has a differentiated solution built for runtime security, namely, KubeArmor (opensource, now a part of CNCF sandbox project) which leverage eBPF for observability of App Behavior and LSMs for enforcement/ in-line mitigation from unknown Zero Day attacks.

Code to Cloud Security

AccuKnox AppSec offers a unique solution, seamlessly integrating open source and commercial security scanning tools. Our flexible security posture approach efficiently prioritizes critical vulnerabilities, ensuring a comprehensive protection journey from code to cloud.

CHAPTER 1

Zero Trust

- Why Zero Trust
- History of Zero Trust
- Definition of Zero Trust
- Government Recommendations

Notable Cloud Breaches

The bigger you are, the bigger the hack.

A day does not go by when we don't hear about major cyber attacks against Cloud Assets. Given that the workloads are moving to the cloud at rapid rate it is only natural that attacks are shifting to the cloud. In addition to the number of attacks the severity and sophistication of the attacks in the cloud are also very advanced.

The Global Cloud Computing Market Size Is Estimated To

Be Valued At
$405.29 Billion
in 2022

And Reach
$1,465.81 Billion
by 2028

With CAGR of
23.9%
by 2028

TESLA

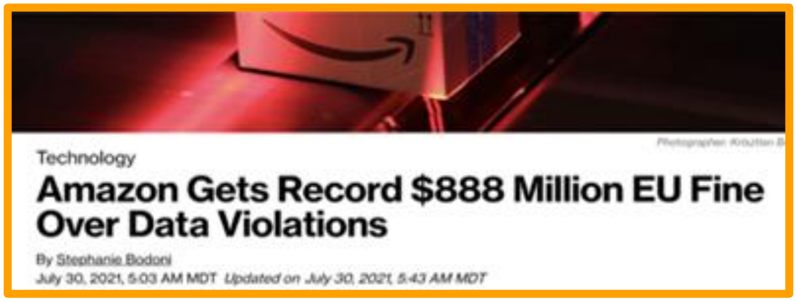
Kubernetes console was vulnerable, and hackers were able to take control and find the credentials to AWS cloud. They were able to gain access to S3 buckets with sensitive data, as well as run cryptocurrency mining in Kubernetes pods.

weight watchers

An insecure Kubernetes cluster console was found by scanning publicly available IPs on kubelet TCP port 10250.

shopify

Exploited containers allowed attackers to overwrite host runc library and gain root access to the container hosts



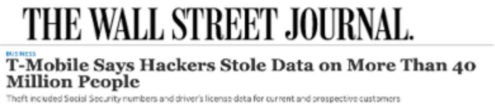
Photographer: Krisztian B

Technology

Amazon Gets Record $888 Million EU Fine Over Data Violations

By Stephanie Bodoni
July 30, 2021, 5:03 AM MDT *Updated on July 30, 2021, 5:43 AM MDT*

T Mobile



THE WALL STREET JOURNAL.

BUSINESS

T-Mobile Says Hackers Stole Data on More Than 40 Million People

Theft included Social Security numbers and driver's license data for current and prospective customers

Key Takeaway

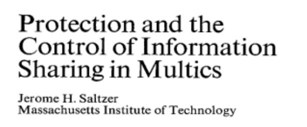
It is only logical that attackers will be increasing the volume, velocity and sophistication of their cyber attacks. Hence it is prudent to instill pertinent security measures.

Revolutionizing Security –
The Timely Renaissance of Zero Trust

Despite being conceived in 1974 with the introduction of Least Privilege, the true potential of Zero Trust principles only emerged a decade ago. It took the impactful SolarWinds breach to propel Zero Trust into mainstream acceptance. This transformative approach shifts the security paradigm from merely thwarting the bad to recognizing the good – a philosophy embodied by Zero Trust.

1974

MIT professor, Saltzer coins the term "Least privilege" Every program should operate using the least set of privileges necessary to complete the job.



Protection and the Control of Information Sharing in Multics

Jerome H. Saltzer
Massachusetts Institute of Technology

1977

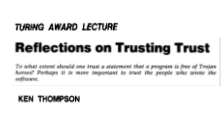
PKI

RSA (Rivest Shamir Adelman), Diffie-Helman Invent public key infrastructure (PKI)

(PKI) is a needed to manage digital certificates and manage public-key encryption. Required for activities where simple passwords are an inadequate and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.

1984

MIT Professor Ken Thompson delivers a seminal lecture on **Trusting Trust**



TURING AWARD LECTURE

Reflections on Trusting Trust

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

KEN THOMPSON

2003

UK Royal Mail organizes Jericho Forum where a new term **DE-PERIMETERIZATION** is introduced

Security Must:

1. Be specific to the asset being protected
2. Pervasive, simple and scalable
3. Leverage Open Protocols
4. Transparent
5. Portable
6. Allow for separation of duties
7. Apply at rest, in transit and in use

2010

John Kindervag, Forrester coins the term <u>Zero Trust</u>

Tenets

1. Network is assumed to be hostile
2. Threat actors are in your network
3. Network segmentation is not enough
4. Policies must be dynamic
5. Device is no longer at the border
6. Containers, Serverless and Cloud are new disruptors

2019

SolarWinds leveraged for several high-profile breaches.

CISA issues Emergency Directive 21-01 "The compromise of SolarWinds' Orion Network Management Products poses unacceptable risks to the security of federal networks," said CISA Acting Director Brandon Wales.

Focus

Remote work has accelerated Zero Trust adoption, with 81% of organizations implementing or considering Zero Trust initiatives to secure remote access.

Zero Trust Tenets

1. The network is always assumed to be hostile
2. Assume threat actors are already inside your network
3. Network locality (segmentation) is not sufficient for deciding trust in a network
4. Every device, user and network flow is authenticated and authorized
5. Policies must be dynamic and calculated from as many sources of data as possible
6. The device is no longer the border. A user/service' identity is the net border
7. Containers, serverless and cloud are the new disruptors of traditional security architecture

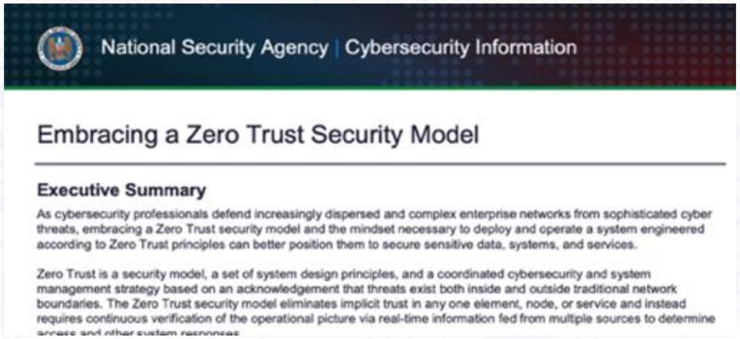
ZERO TRUST ADAGE
Verify, Then Trust, Continuously Verify

"If organizations don't adapt to the new development and adopt the Zero Trust principles, "they probably will be going out of business in this digital world."

July 2023

pwc

Zero Trust Devices, Networks and Users



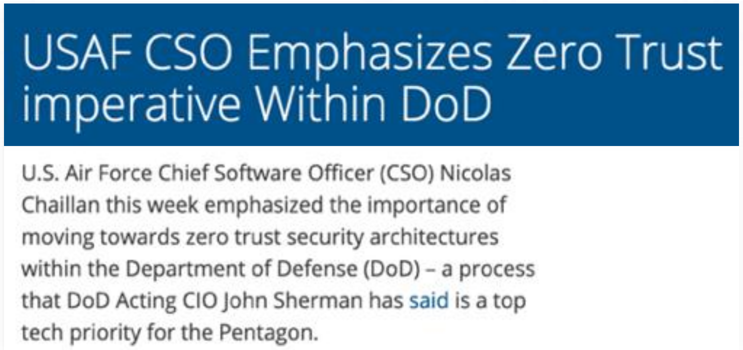
National Security Agency | Cybersecurity Information

Embracing a Zero Trust Security Model

Executive Summary

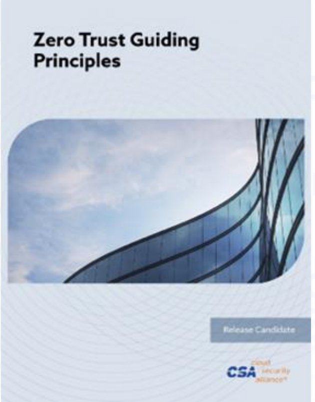
As cybersecurity professionals defend increasingly dispersed and complex enterprise networks from sophisticated cyber threats, embracing a Zero Trust security model and the mindset necessary to deploy and operate a system engineered according to Zero Trust principles can better position them to secure sensitive data, systems, and services.

Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information fed from multiple sources to determine access and other system responses

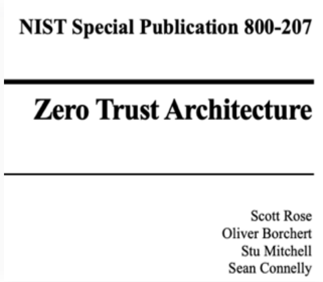


USAF CSO Emphasizes Zero Trust imperative Within DoD

U.S. Air Force Chief Software Officer (CSO) Nicolas Chaillan this week emphasized the importance of moving towards zero trust security architectures within the Department of Defense (DoD) – a process that DoD Acting CIO John Sherman has said is a top tech priority for the Pentagon.



Zero Trust Guiding Principles



NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

Newsflash

Zero Trust is not an entirely new idea. The concept of least privilege has been around for a long time. However, the recent Zero Day attacks has brought board room visibility to this.

CHAPTER 2

Zero Trust CNAPP

1 Why Zero Trust CNAPP?

2 CNAPP

3 CSPM, KSPM – Cloud, Kubernetes Posture Management

4 ASPM – Application Security Posture Management

5 CIEM, KIEM – Cloud, K8 Identity Entitlement Mgmt

6 Zero Trust – Defense in Depth

7 GRC – Governance, Risk and Compliance

8 Integration

9 Deployment

10 Leveraging AI

Ephemeral and Transient Nature of Containers

ISACA Silicon Valley Chapter

EVOLUTION OF SERVER WORKLOAD ABSTRACTIONS

PHYSICAL

- Monolithic applications
- Physical servers as unit of scaling
- Life span of years

VIRTUAL MACHINES

- Hardware virtualization
- VMs as unit of scaling
- Life span of months to years

CONTAINERS

- OS Virtualization
- Applications/services as unit of scaling
- **Lifespan of minutes to days**

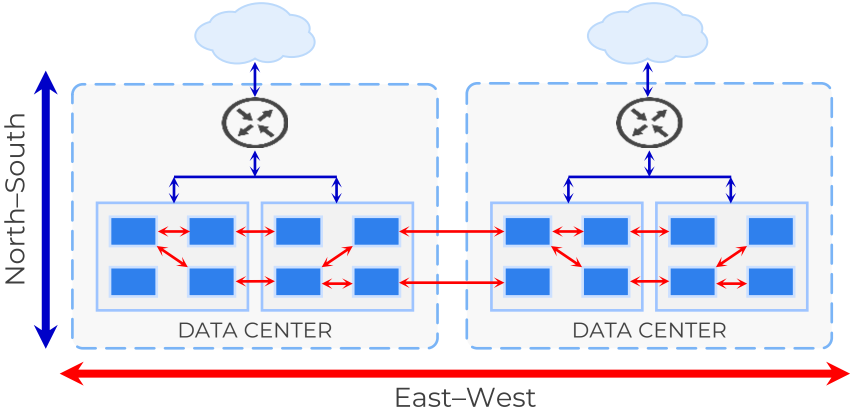
SERVERLESS

Lifespan of seconds to minutes

UNMONITORED INTER-CONTAINER COMMUNICATION

Current
Container Security Solutions
Do not have a mechanism to **affirmatively enforce Policy Compliance**

Current
Perimeter Defenses
Firewalls, End Point
address only North-South
[17% of the traffic]



Source: Gartner 2019

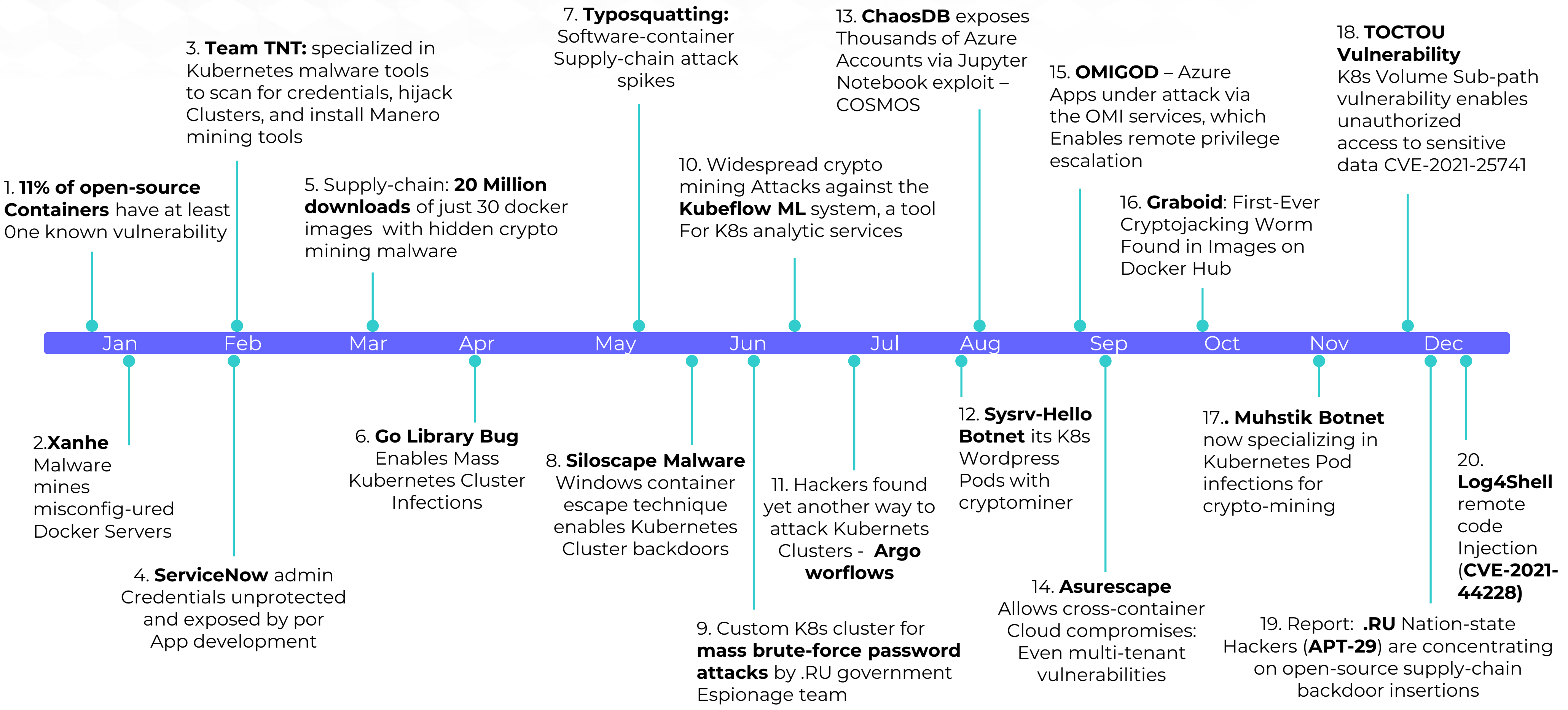
Beware

Almost all modern Zero Day threats originate in un-monitored East-West, lateral movement attack vectors.

WHAT PROBLEM DOES CNAPP SOLVE?

Overcoming Inadequacy of Traditional Perimeter Defenses Against Sophisticated Cloud Attacks

Top 20 Cloud Security Incidents In 2021



1. **11% of open-source Containers** have at least 0ne known vulnerability

2.**Xanhe** Malware mines misconfig-ured Docker Servers

3. **Team TNT:** specialized in Kubernetes malware tools to scan for credentials, hijack Clusters, and install Manero mining tools

4. **ServiceNow** admin Credentials unprotected and exposed by por App development

5. Supply-chain: **20 Million downloads** of just 30 docker images with hidden crypto mining malware

6. **Go Library Bug** Enables Mass Kubernetes Cluster Infections

7. **Typosquatting:** Software-container Supply-chain attack spikes

8. **Siloscape Malware** Windows container escape technique enables Kubernetes Cluster backdoors

9. Custom K8s cluster for **mass brute-force password attacks** by .RU government Espionage team

10. Widespread crypto mining Attacks against the **Kubeflow ML** system, a tool For K8s analytic services

11. Hackers found yet another way to attack Kubernets Clusters - **Argo worflows**

12. **Sysrv-Hello Botnet** its K8s Wordpress Pods with cryptominer

13. **ChaosDB** exposes Thousands of Azure Accounts via Jupyter Notebook exploit – COSMOS

14. **Asurescape** Allows cross-container Cloud compromises: Even multi-tenant vulnerabilities

15. **OMIGOD** – Azure Apps under attack via the OMI services, which Enables remote privilege escalation

16. **Graboid**: First-Ever Cryptojacking Worm Found in Images on Docker Hub

17.. **Muhstik Botnet** now specializing in Kubernetes Pod infections for crypto-mining

18. **TOCTOU Vulnerability** K8s Volume Sub-path vulnerability enables unauthorized access to sensitive data CVE-2021-25741

19. Report: **.RU** Nation-state Hackers (**APT-29**) are concentrating on open-source supply-chain backdoor insertions

20. **Log4Shell** remote code Injection (**CVE-2021-44228)**

https://blog.accuknox.com/2021-cloud-security-year-end-review/

Brilliant Idea

“Average Time to Detect and Respond to Security Incidents” is a crucial metric. It indicates the effectiveness of security operations in identifying and addressing potential threats.

WHAT PROBLEM DOES CNAPP SOLVE?

Addressing the Limitations of Simple Perimeter Defenses in the Face of Advanced Cloud Threats

Top 20 Cloud Security Incidents In 2022

1. **11% of open-source containers** have at least one know vulnerabilities
2. **Xanhe** Malware mines misconfigured Docker Servers
3. **Team TNT:** Specialized in Kubernetes malware tools to scan for credentials, hijack Cluster & Install Manero
4. **ServiceNow admin credentials unprotected** & exposed by pro App development
5. **Supply-chain: 20 Million downloads** of just 30 docker images with hidden crypto mining malware
6. **Go Library Bug** Enables Mass Kubernetes Cluster Infections
7. **Typosquatting:** Software-container **Supply-chain attack spikes**
8. **Siloscape Malware Windows** container Escape technique Enables Kubernetes Cluster backdoors
9. Custom K8s cluster for **mass brute-force password attacks** by .RU government Espionage team
10. Widespread crypto mining attacks against the **Kubeflow ML** system, a tool for K8s analytic services.
11. Hackers found Yet another way To attack Kubernetes Clusters - **Argo workflows**
12. **Sysrv-Hello Botnet** its K8s Wordpress Pods with cryptominer
13. **ChaosDB** exposes Thousands of Azure Accounts via Jupyter Notebook exploit – COSMOS
14. **Asurescape** Allows cross-container Cloud compromises: Even multi tenant vulnerabilities
15. **OMIGOD** – Azure Apps under attack via the OMI services, which Enables remote privilege escalation
16. **Graboid:** First-Ever Cryptojacking Worm Found in Images on Docker Hub
17. **Muhstik Botnet** now specializing in Kubernetes Pod infections for crypto-mining
18. **TOCTOU** Vulnerability K8s Volume Sub-path vulnerability enables unauthorized access to sensitive data CVE-2021-25741
19. Report: **.RU** Nation-state Hackers (**APT-29**) are concentrating on open-source supply-chain backdoor insertions
20. **Log4Shell remote code Injection** (CVE-2021-44228)

Key Takeaway

Inline mitigation is critical for real-time threat interception and neutralization, improving security posture by preventing breaches and lowering the risk of successful attacks.

How CNAPP Neutralizes Advanced Threats?

ZERO-DAY ATTACKS ROOT CAUSES	ZERO TRUST MITIGATION APPROACHES
Privilege escalation	Run-time Security
Lateral movement	Micro-segmentation
Process subversion	Application Firewalling
Rootkit attacks	Kernel Hardening
Embedded malicious logic	In-line Security
Unauthorized file system manipulations	
Malicious network interface usage	
Unauthorized process execution, termination, thread hijacking	
Unauthorized administrative functions and command invocation	

Beware

Zero-day attacks require proactive security measures, continuous monitoring, and rapid response to protect sensitive information and organizational integrity from unauthorized access, data breaches, and financial losses.

CNAPP – Cloud Native Application Protection Platform

Gartner

Market Guide for Cloud-Native Application Protection Platforms

Gartner

Market Guide for Cloud-Native Application Protection Platforms

Published 14 March 2023 - ID G00785751 - 28 min read

By Neil MacDonald, Charlie Winckless, Dale Koeppen

Initiatives: Security of Applications and Data; Infrastructure Security

CNAPPs address the full life cycle protection requirements of cloud-native applications from development to production. Security and risk management leaders responsible for cloud security strategies should use this research to analyze and evaluate emerging CNAPP offerings.

- ✓ **Integrated Security Lifecycle** - Implement a holistic approach to secure cloud-native applications, spanning from development to runtime protection.
- ✓ **Developer Toolchain Integration** - Integrate security seamlessly into the developer's toolchain, automating testing throughout the development pipeline to enhance adoption efficiency.
- ✓ **Focus on Critical Vulnerabilities** - Prioritize the identification and remediation of highest severity, highest confidence, and highest risk vulnerabilities, optimizing developer efforts.
- ✓ **Comprehensive Artifact and Configuration Scanning** - Conduct thorough scans of development artifacts and cloud configurations, coupled with runtime visibility, to prioritize and remediate security risks effectively.
- ✓ **Diverse Runtime Visibility Techniques** - Choose CNAPP vendors offering a range of runtime visibility techniques, including traditional agents, eBPF support, snapshotting, privileged containers, and Kubernetes integration for deployment flexibility.

AccuKnox Zero Trust CNAPP meets all the guidelines outlined by Gartner

Certify-Verify

Cloud-native apps require automated testing. Prioritize critical vulnerabilities, and diverse runtime visibility for robust protection. Security should be dynamic and responsive to changes in the cloud environment.

CNAPP – Cloud Native Application Protection Platform

AccuKnox Enterprise CNAPP Suite

Shift Left Defense

- Thwart advanced "Zero Day" attacks with a proactive Shift Left approach.

Security Layers:

- Static Security: Leverage Cloud Security Posture Management (CSPM).
- Run-time Security: Utilize Cloud Workload Protection Platform (CWPP).

Integrated Testing

- Seamlessly integrate with Static Application Security Testing (SAST), Software Composition Analysis (SCA), and API Protection (DAST).

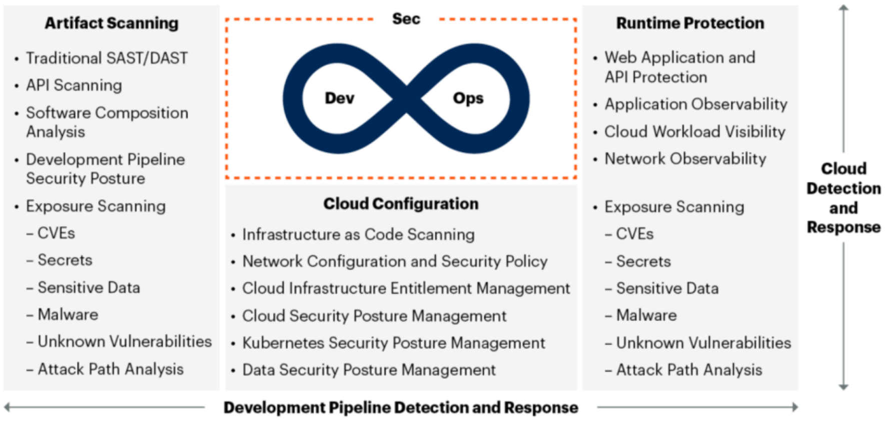
Identity Management:

- Cloud Identity and Entitlement Management (CIEM).
- Kubernetes Identity and Entitlement Management (KIEM).

Real-Time Protection

- Stay one step ahead with real-time defense against zero-day attacks.

CNAPP Detailed View



Artifact Scanning

- Traditional SAST/DAST
- API Scanning
- Software Composition Analysis
- Development Pipeline Security Posture
- Exposure Scanning
  - CVEs
  - Secrets
  - Sensitive Data
  - Malware
  - Unknown Vulnerabilities
  - Attack Path Analysis

Sec

Dev Ops

Cloud Configuration

- Infrastructure as Code Scanning
- Network Configuration and Security Policy
- Cloud Infrastructure Entitlement Management
- Cloud Security Posture Management
- Kubernetes Security Posture Management
- Data Security Posture Management

Runtime Protection

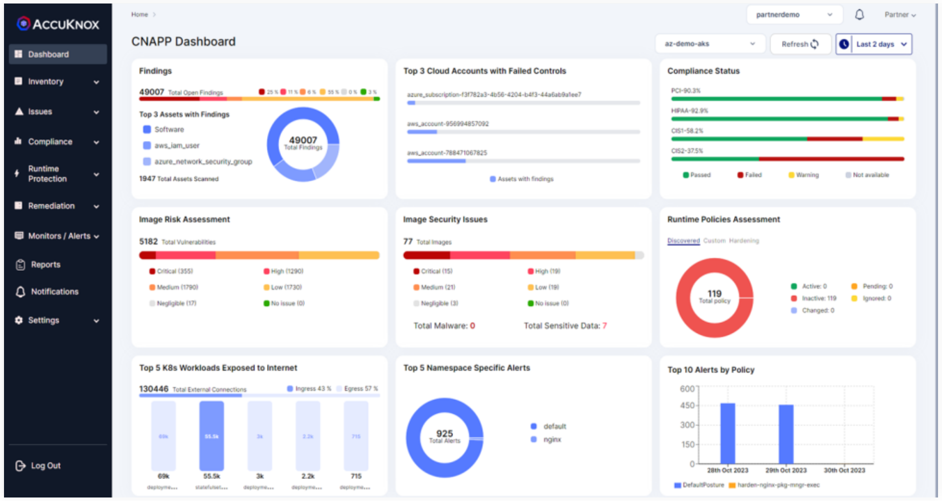
- Web Application and API Protection
- Application Observability
- Cloud Workload Visibility
- Network Observability
- Exposure Scanning
  - CVEs
  - Secrets
  - Sensitive Data
  - Malware
  - Unknown Vulnerabilities
  - Attack Path Analysis

Cloud Detection and Response

Development Pipeline Detection and Response

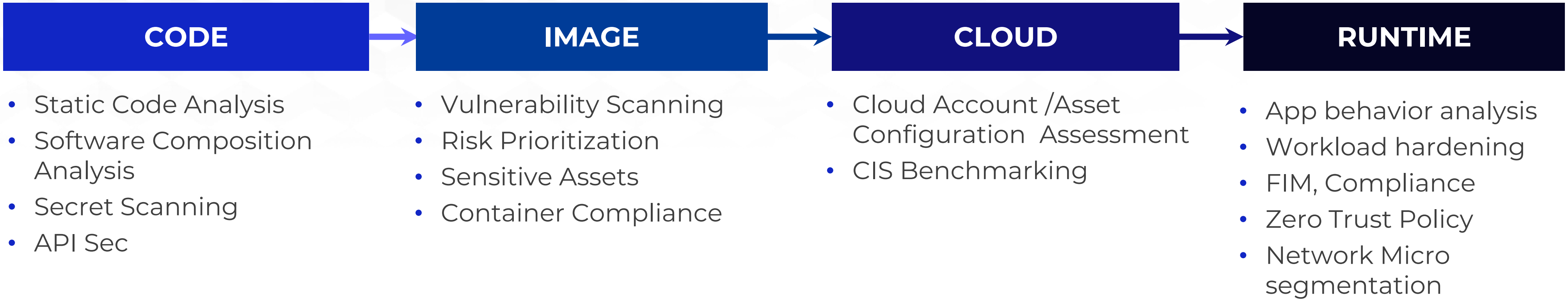
CVEs = common vulnerabilities and exposures

Source: Gartner



Strategy One needs to take a comprehensive and holistic approach to cloud security. Fragmented and disjointed approaches results in “alert deluge”, inefficient and ineffective security operations.

Zero Trust Security From Code → Cloud



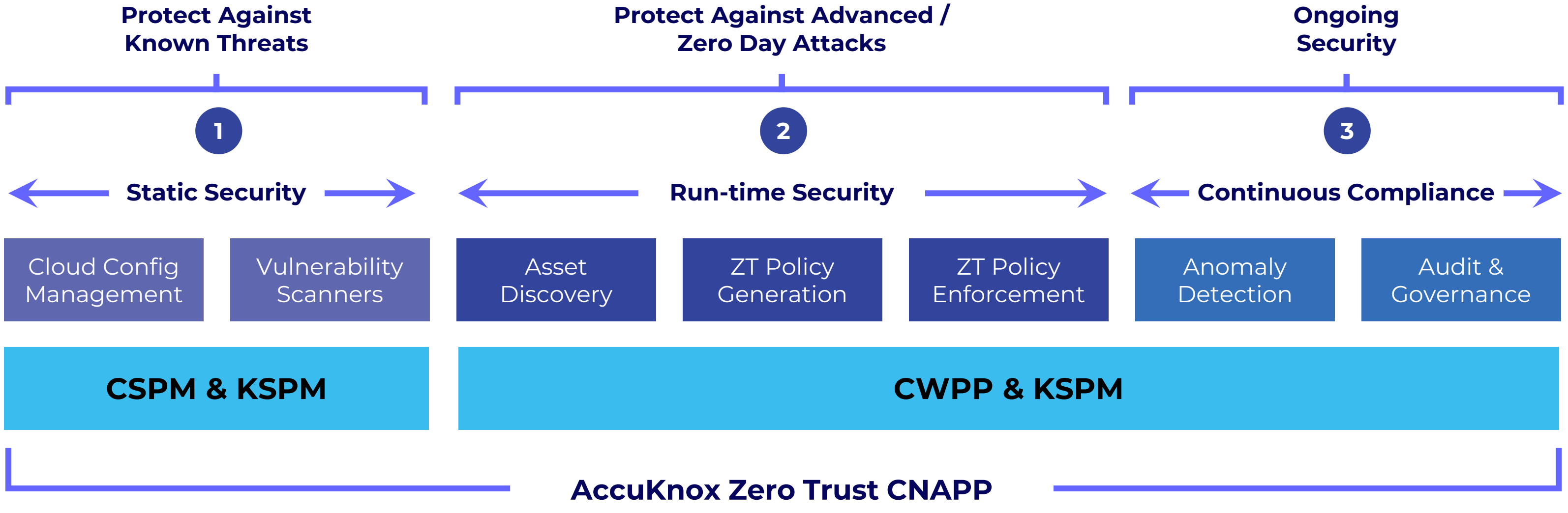
CODE → **IMAGE** → **CLOUD** → **RUNTIME**

CODE
- Static Code Analysis
- Software Composition Analysis
- Secret Scanning
- API Sec

IMAGE
- Vulnerability Scanning
- Risk Prioritization
- Sensitive Assets
- Container Compliance

CLOUD
- Cloud Account /Asset Configuration Assessment
- CIS Benchmarking

RUNTIME
- App behavior analysis
- Workload hardening
- FIM, Compliance
- Zero Trust Policy
- Network Micro segmentation



Protect Against Known Threats
1 Static Security
- Cloud Config Management
- Vulnerability Scanners

Protect Against Advanced / Zero Day Attacks
2 Run-time Security
- Asset Discovery
- ZT Policy Generation
- ZT Policy Enforcement

Ongoing Security
3 Continuous Compliance
- Anomaly Detection
- Audit & Governance

CSPM & KSPM

CWPP & KSPM

AccuKnox Zero Trust CNAPP

Technical Stuff

Cloud-native apps require automated testing. Prioritize critical vulnerabilities, and diverse runtime visibility for robust protection. Security should be dynamic and responsive to changes in the cloud environment.

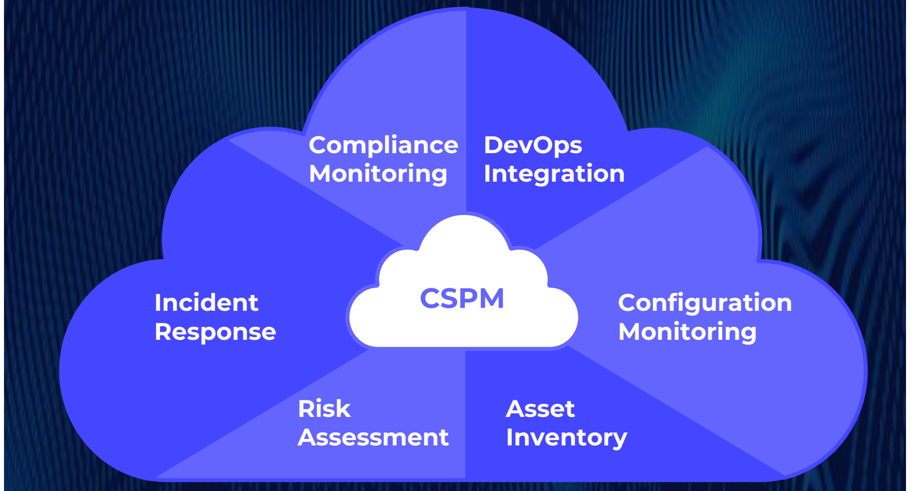
CSPM – Cloud Security Posture Management

CSPM – Definition, Features, and Dashboard

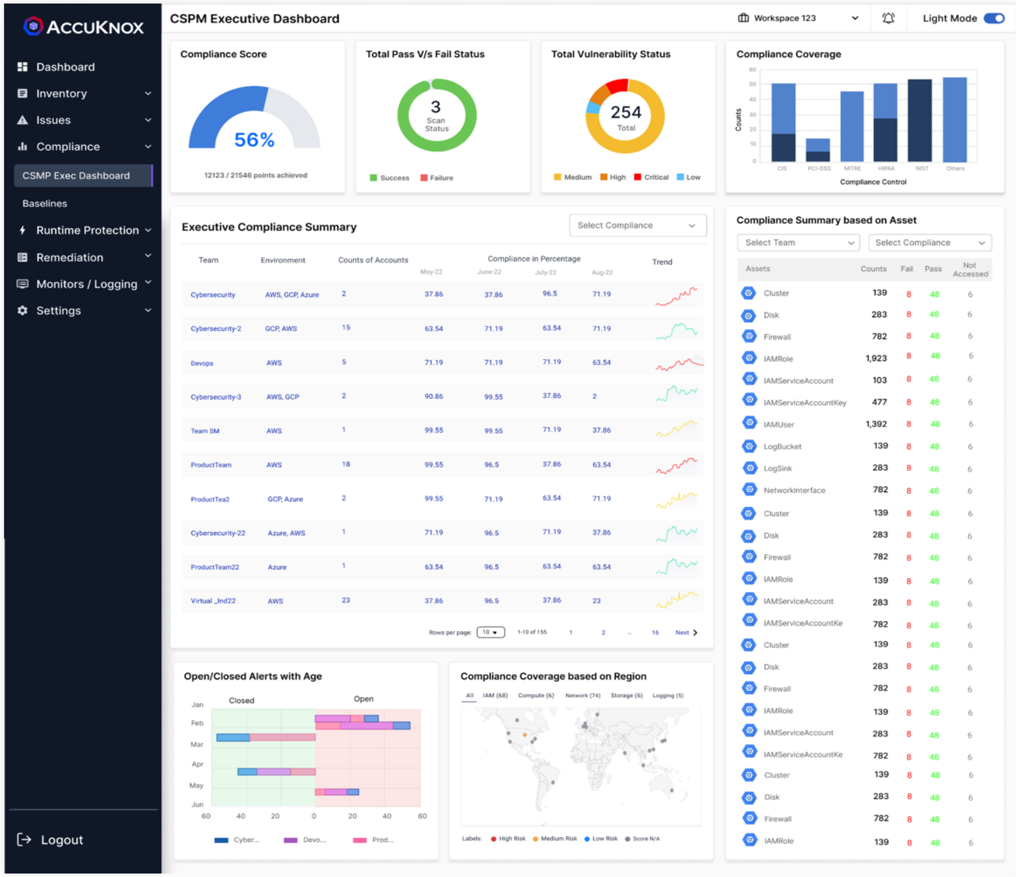
Gartner

Gartner Defines CSPM As

“A continuous process of cloud security improvement and adaptation to reduce the likelihood of a successful attack”



Core Capabilities of CSPM



CSPM Executive Dashboard

12123 / 21546 points achieved

Executive Compliance Summary

Select Compliance

Team	Environment	Counts of Accounts	Compliance in Percentage May-22	June-22	July-22	Aug-22	Trend
Cybersecurity	AWS, GCP, Azure	2	37.86	37.86	96.5	71.19	
Cybersecurity-2	GCP, AWS	15	63.54	71.19	63.54	71.19	
Devops	AWS	5	71.19	71.19	71.19	63.54	
Cybersecurity-3	AWS, GCP	2	90.86	99.55	37.86	2	
Team SM	AWS	1	99.55	99.55	71.19	37.86	
ProductTeam	AWS	18	99.55	96.5	37.86	63.54	
ProductTea2	GCP, Azure	2	99.55	71.19	63.54	71.19	
Cybersecurity-22	Azure, AWS	1	71.19	96.5	71.19	37.86	
ProductTeam22	Azure	1	63.54	96.5	63.54	63.54	
Virtual _Ind22	AWS	23	37.86	96.5	37.86	23	

Rows per page: 10 ▾ 1-10 of 155 1 2 ... 16 Next ›

Compliance Summary based on Asset

Select Team ⌄ Select Compliance ⌄

Assets	Counts	Fail	Pass	Not Accessed
Cluster	139	8	48	6
Disk	283	8	48	6
Firewall	782	8	48	6
IAMRole	1,923	8	48	6
IAMServiceAccount	103	8	48	6
IAMServiceAccountKey	477	8	48	6
IAMUser	1,392	8	48	6
LogBucket	139	8	48	6
LogSink	283	8	48	6
NetworkInterface	782	8	48	6
Cluster	139	8	48	6
Disk	283	8	48	6
Firewall	782	8	48	6
IAMRole	139	8	48	6
IAMServiceAccount	283	8	48	6
IAMServiceAccountKe	782	8	48	6
Cluster	139	8	48	6
Disk	283	8	48	6
Firewall	782	8	48	6
IAMRole	139	8	48	6
IAMServiceAccount	283	8	48	6
IAMServiceAccountKe	782	8	48	6
Cluster	139	8	48	6
Disk	283	8	48	6
Firewall	782	8	48	6
IAMRole	139	8	48	6

Technical Stuff

CSPM, finds and fixes cloud environment misconfigurations. It precisely and efficiently improves security posture and offers proactive remedial recommendations.

CSPM – Cloud Security Posture Management

ACCUKNOX CSPM VALUE ADD OVER WHAT HYPERSCALERS PROVIDE

Multi-cloud support

Analyze Baseline Compliance for All Regions, even unconfigured ones

Review and address findings ignoring repetitive issues, no need to re-review things which have been identified as not being real issues

Allow security analyst to review policies, configuration, and findings without granting console access

Monitor assets for changes to indicate when a re-review is necessary or if an undesirable condition has been detected.

Analyze findings from other sources within context of an asset, i.e. static code analysis results grouped with container findings

Report across groups that represent real world structures (business units, applications, departments, etc.)

Provide reports demonstrating activity to governing agencies or 3PAO

Manage full lifecycle of security processes not just identification

Assess pass/fail and **remember** status producing a true Baseline

Take action on findings by opening tickets with responsible party to resolve

HYPER SCALERS

aws

Analyze Baseline Compliance for All Regions, even unconfigured ones

Generate findings for potential security issues

Perform service specific security analysis (Macie, Analyzer, Detective, etc.)

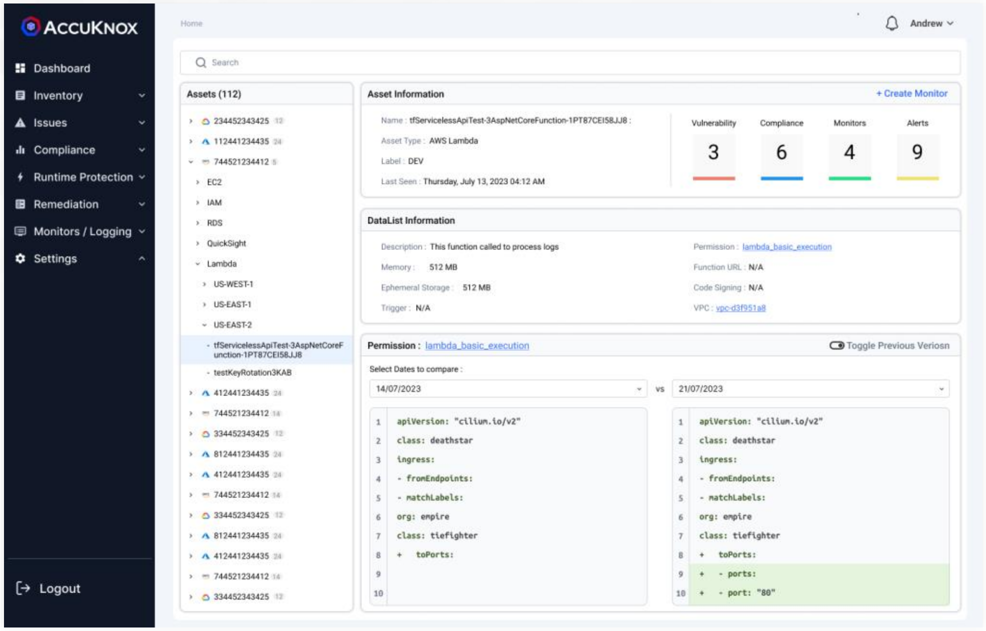
Collect vulnerability data and manage patching

Summary

AccuKnox CSPM tool uses agentless technology to enhance cloud security. It actively identifies and prioritizes vulnerabilities. Easy to achieve compliance with regulations. Tightly coupled integration with SIEM/SOAR platforms.

CSPM – Cloud Security Posture Management

- Asset discovery on Multi-Cloud
- Mapped misconfigurations and vulnerabilities to each asset
- Detect critical assets with highest severity and group findings based on asset
- Group critical assets together and do proactive monitoring for configuration change
- Multi-Cloud Support for Drift Detection
- Full scans generates lot of noise and information that could be redundant
- Baselining Infrastructure with respect to particular controls by CIS, PCI-DSS or multiple data sources that AccuKnox supports
- Delta difference over time will be recorded and generated as an alert
- Provides proactive Monitoring vs Point-in-time snapshot



Asset Information

Name : tfServicelessApiTest-3AspNetCoreFunction-1PT87CEI58JJ8 :

Asset Type : AWS Lambda

Label : DEV

Last Seen : Thursday, July 13, 2023 04:12 AM

Vulnerability	Compliance	Monitors	Alerts
3	6	4	9

DataList Information

Description : This function called to process logs

Memory : 512 MB

Ephemeral Storage : 512 MB

Trigger : N/A

Permission : lambda_basic_execution

Function URL : N/A

Code Signing : N/A

VPC : vpc-d3f951a8

Permission : lambda_basic_execution

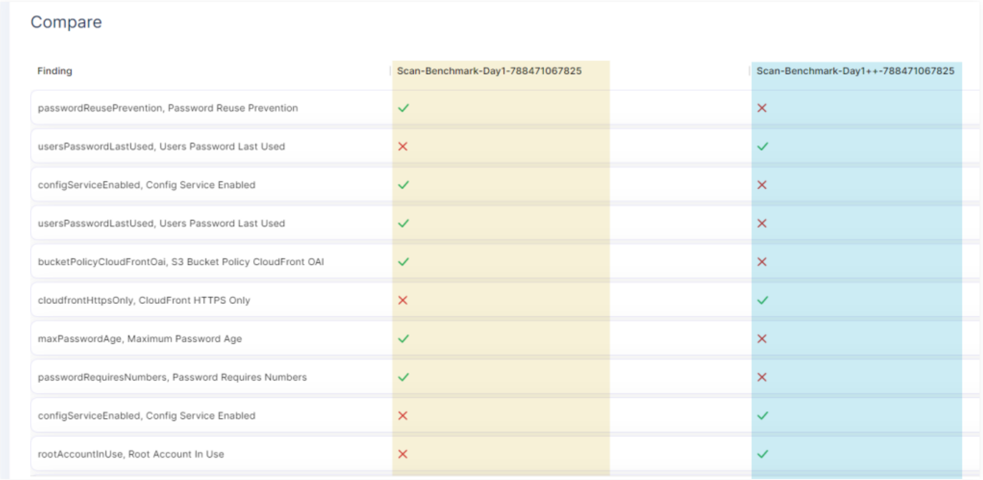
Select Dates to compare :

14/07/2023 vs 21/07/2023

```
apiVersion: "cilium.io/v2"
class: deathstar
ingress:
- fromEndpoints:
- matchLabels:
org: empire
class: tiefighter
+   toPorts:


```

```
apiVersion: "cilium.io/v2"
class: deathstar
ingress:
- fromEndpoints:
- matchLabels:
org: empire
class: tiefighter
+   toPorts:
+   - ports:
+   - port: "80"
```



Compare

Finding	Scan-Benchmark-Day1-788471067825	Scan-Benchmark-Day1++-788471067825
passwordReusePrevention, Password Reuse Prevention	✓	✗
usersPasswordLastUsed, Users Password Last Used	✗	✓
configServiceEnabled, Config Service Enabled	✓	✗
usersPasswordLastUsed, Users Password Last Used	✓	✗
bucketPolicyCloudFrontOai, S3 Bucket Policy CloudFront OAI	✓	✗
cloudfrontHttpsOnly, CloudFront HTTPS Only	✗	✓
maxPasswordAge, Maximum Password Age	✓	✗
passwordRequiresNumbers, Password Requires Numbers	✓	✗
configServiceEnabled, Config Service Enabled	✗	✓
rootAccountInUse, Root Account In Use	✗	✓

Focus

CSPM addresses the basic foundational “must have” elements of Cloud Security. Every organization needs to have one.

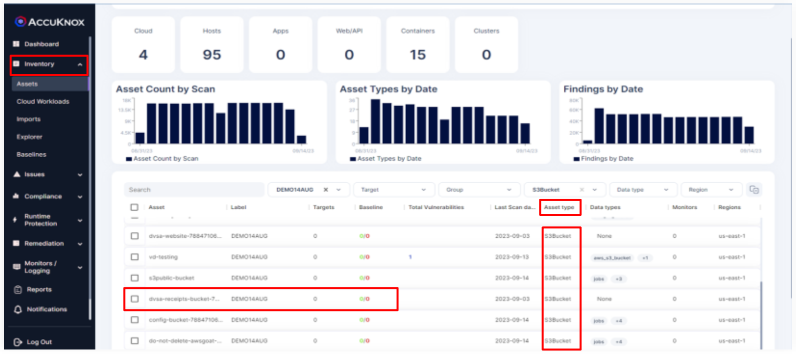
Exposed Treasures

Identifying Publicly Accessible S3 Buckets

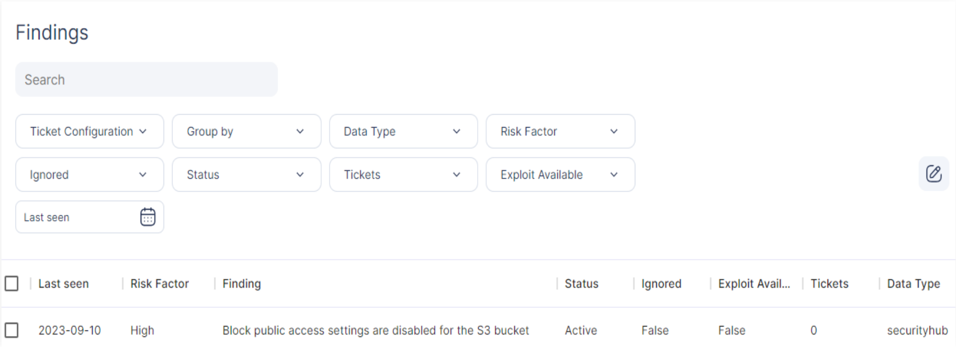
1. Go to Inventory >> Assets page and Filter for Asset Type as **s3bucket**
2. Look for **S3bucket** with count in **Total Vulnerabilities**

After Identification of **S3bucket** with misconfiguration, click on the bucket with misconfiguration(vd-testing) to see the detailed view.

1

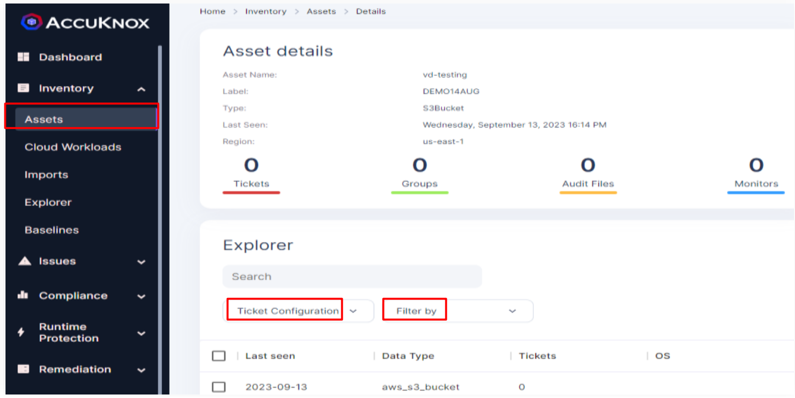


☐	Asset	Label	Targets	Baseline	Total Vulnerabilities	Last Scan da...	Asset type	Data types	Monitors	Regions
☐	dvsa-website-78847106...	DEMO14AUG	0	0/0		2023-09-03	S3Bucket	None	0	us-east-1
☐	vd-testing	DEMO14AUG	0	0/0	1	2023-09-13	S3Bucket	aws_s3_bucket +1	0	us-east-1
☐	s3public-bucket	DEMO14AUG	0	0/0		2023-09-14	S3Bucket	jobs +3	0	us-east-1
☐	dvsa-receipts-bucket-7...	DEMO14AUG	0	0/0		2023-09-03	S3Bucket	None	0	us-east-1
☐	config-bucket-78847106...	DEMO14AUG	0	0/0		2023-09-14	S3Bucket	jobs +4	0	us-east-1
☐	do-not-delete-awsgoat-...	DEMO14AUG	0	0/0		2023-09-14	S3Bucket	jobs +4	0	us-east-1



☐	Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets	Data Type
☐	2023-09-10	High	Block public access settings are disabled for the S3 bucket	Active	False	False	0	securityhub

2



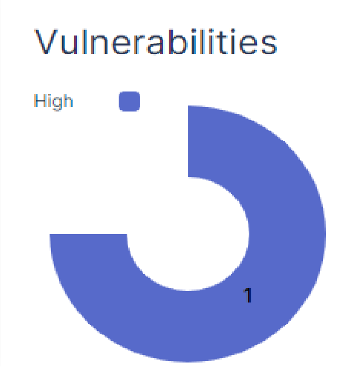
Asset details

Asset Name: vd-testing
Label: DEMO14AUG
Type: S3Bucket
Last Seen: Wednesday, September 13, 2023 16:14 PM
Region: us-east-1

0 Tickets · 0 Groups · 0 Audit Files · 0 Monitors

Explorer

☐	Last seen	Data Type	Tickets	OS
☐	2023-09-13	aws_s3_bucket	0	



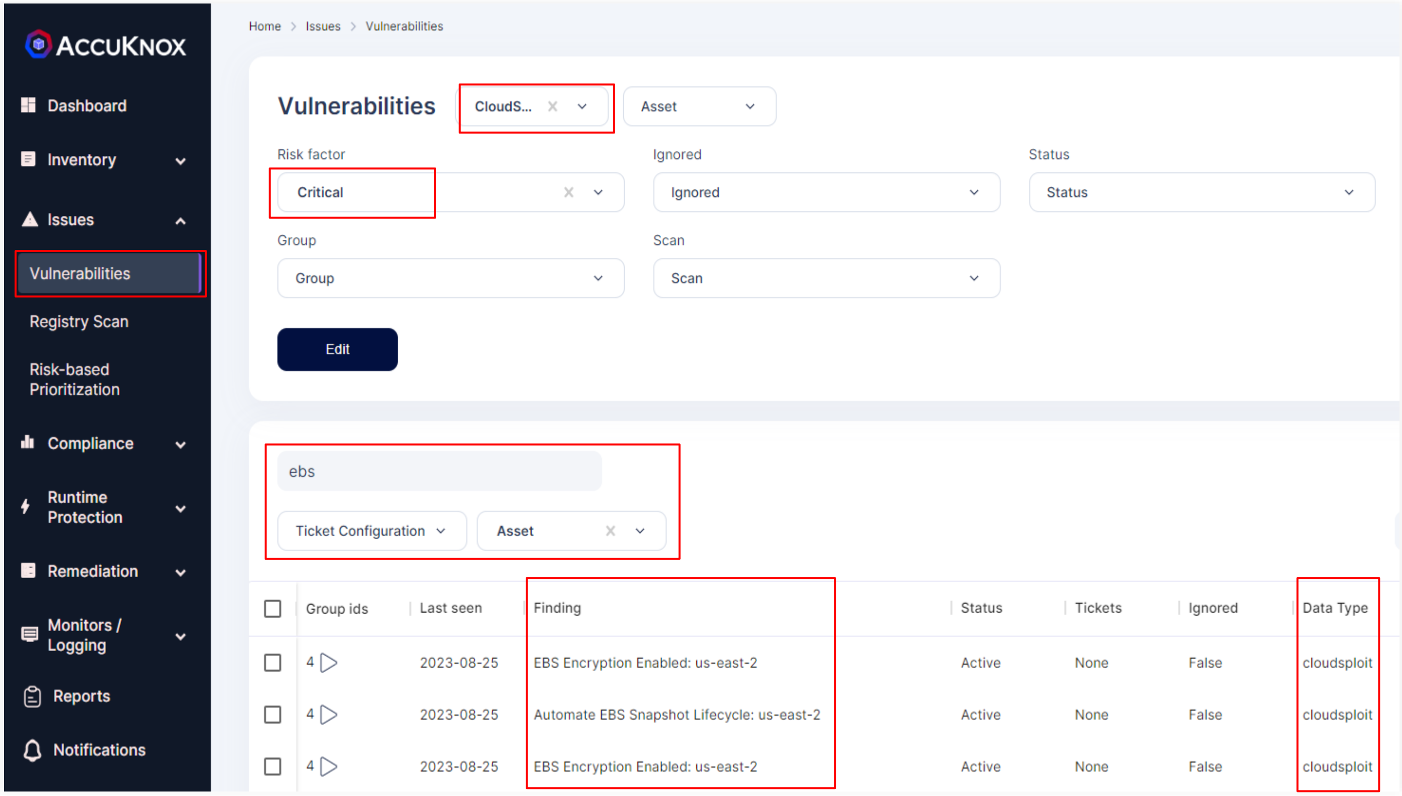
Considerations

Implement an automated monitoring system for S3 bucket changes. Regularly audit permissions using AWS Config Rules. Promptly identify and rectify potential data leaks.

Spotting Unencrypted EBS Volumes

To identify the unencrypted EBS Volume associated with the Onboarded Cloud Account, please navigate to Issues → Vulnerabilities

- Apply **Cloudsploit** in data-type filter
- Choose the severity “Critical” for the Findings
- Search for “ebs volume” in the search field



Vulnerabilities

CloudS... | Asset

Risk factor: Critical

Ignored: Ignored

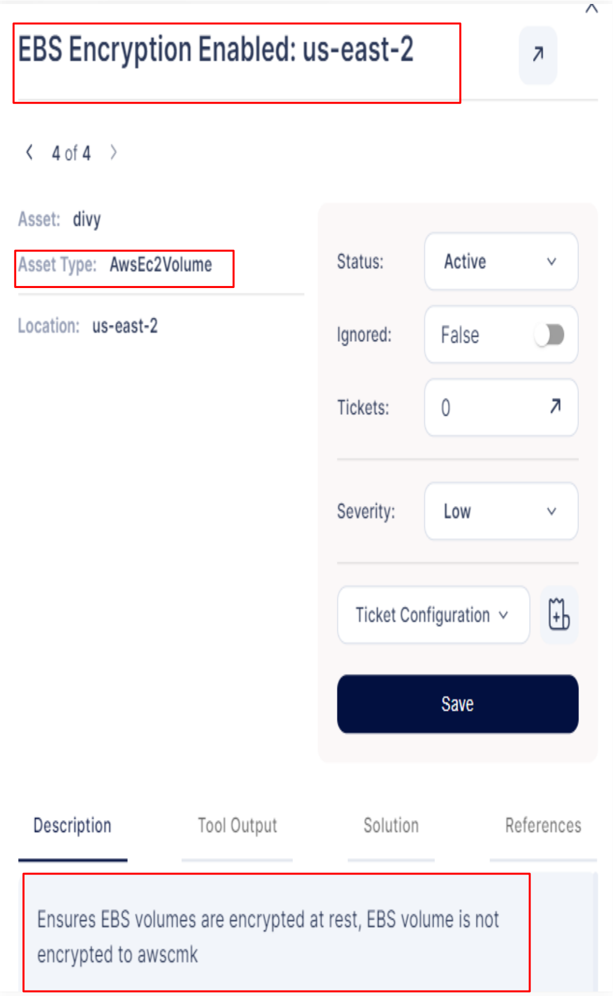
Status: Status

Group: Group

Scan: Scan

ebs

Group ids	Last seen	Finding	Status	Tickets	Ignored	Data Type
4	2023-08-25	EBS Encryption Enabled: us-east-2	Active	None	False	cloudsploit
4	2023-08-25	Automate EBS Snapshot Lifecycle: us-east-2	Active	None	False	cloudsploit
4	2023-08-25	EBS Encryption Enabled: us-east-2	Active	None	False	cloudsploit



EBS Encryption Enabled: us-east-2

4 of 4

Asset: divy

Asset Type: AwsEc2Volume

Location: us-east-2

Status: Active

Ignored: False

Tickets: 0

Severity: Low

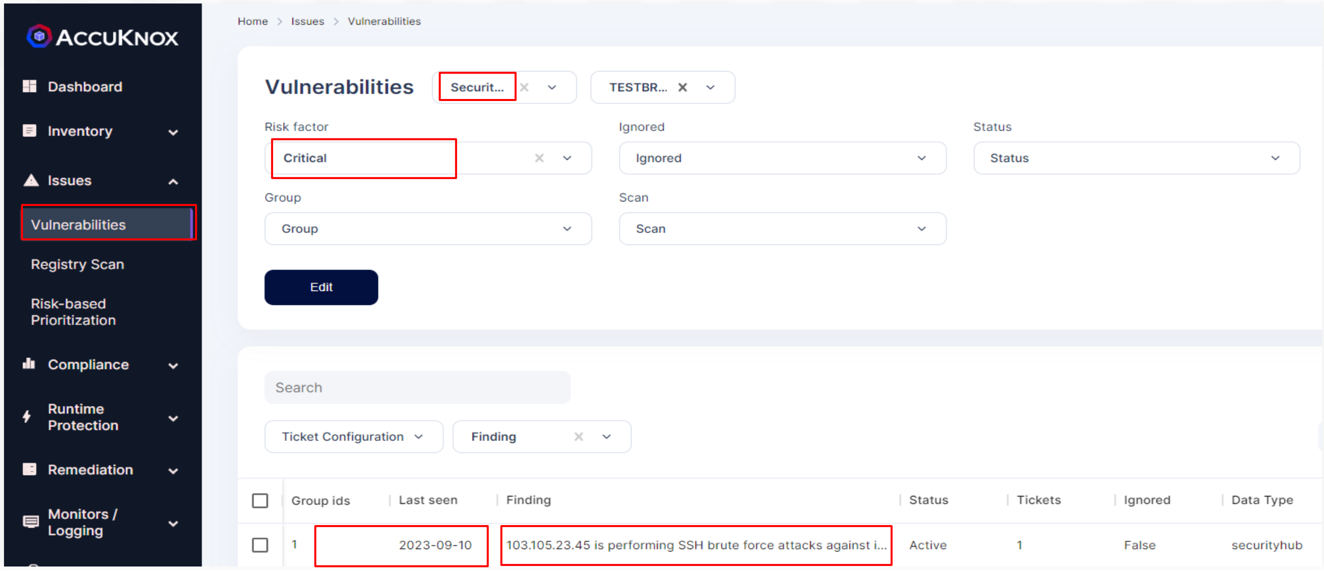
Ensures EBS volumes are encrypted at rest, EBS volume is not encrypted to awscmk

Focus Cloudsploit’s robust data-type filtering and granular search capabilities enable the easy identification of critical vulnerabilities. Streamlining security measures and protecting cloud infrastructure against potential risks is simple as it gets.

Identify Hosts with Critical Findings

To identify Hosts with the Critical Findings, Please navigate to Issues → Vulnerabilities

- Apply **SecurityHub** in data-type filter
- Choose the severity "Critical" for the Findings



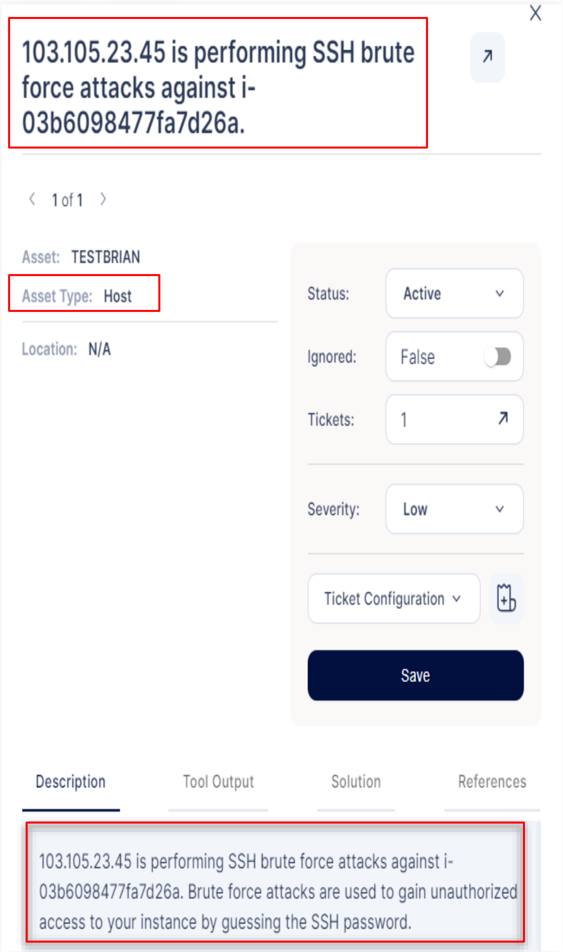
Vulnerabilities — Securit... × | TESTBR... ×

Risk factor: Critical | Ignored: Ignored | Status: Status

Group: Group | Scan: Scan

Ticket Configuration | Finding ×

☐	Group ids	Last seen	Finding	Status	Tickets	Ignored	Data Type
☐	1	2023-09-10	103.105.23.45 is performing SSH brute force attacks against i...	Active	1	False	securityhub



103.105.23.45 is performing SSH brute force attacks against i-03b6098477fa7d26a.

Asset: TESTBRIAN

Asset Type: Host

Location: N/A

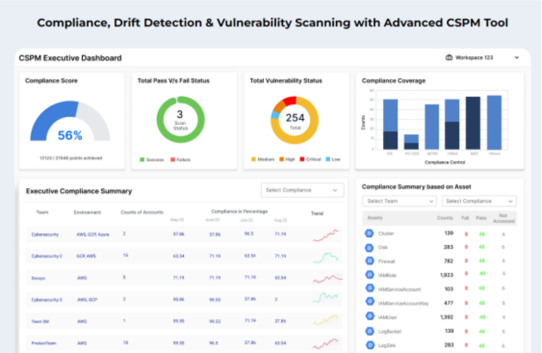
Status: Active

Ignored: False

Tickets: 1

Severity: Low

103.105.23.45 is performing SSH brute force attacks against i-03b6098477fa7d26a. Brute force attacks are used to gain unauthorized access to your instance by guessing the SSH password.


Compliance, Drift Detection & Vulnerability Scanning with Advanced CSPM Tool
CSPM Executive Dashboard
Compliance Score
56%
Total Pass V/s Fail Status
3
Total Vulnerability Status
254
Compliance Coverage
Executive Compliance Summary
Compliance Summary based on Asset

The global market for CSPM is projected to grow at a CAGR of 15.3% from $4.2 billion in 2022 to $8.6 billion by 2027

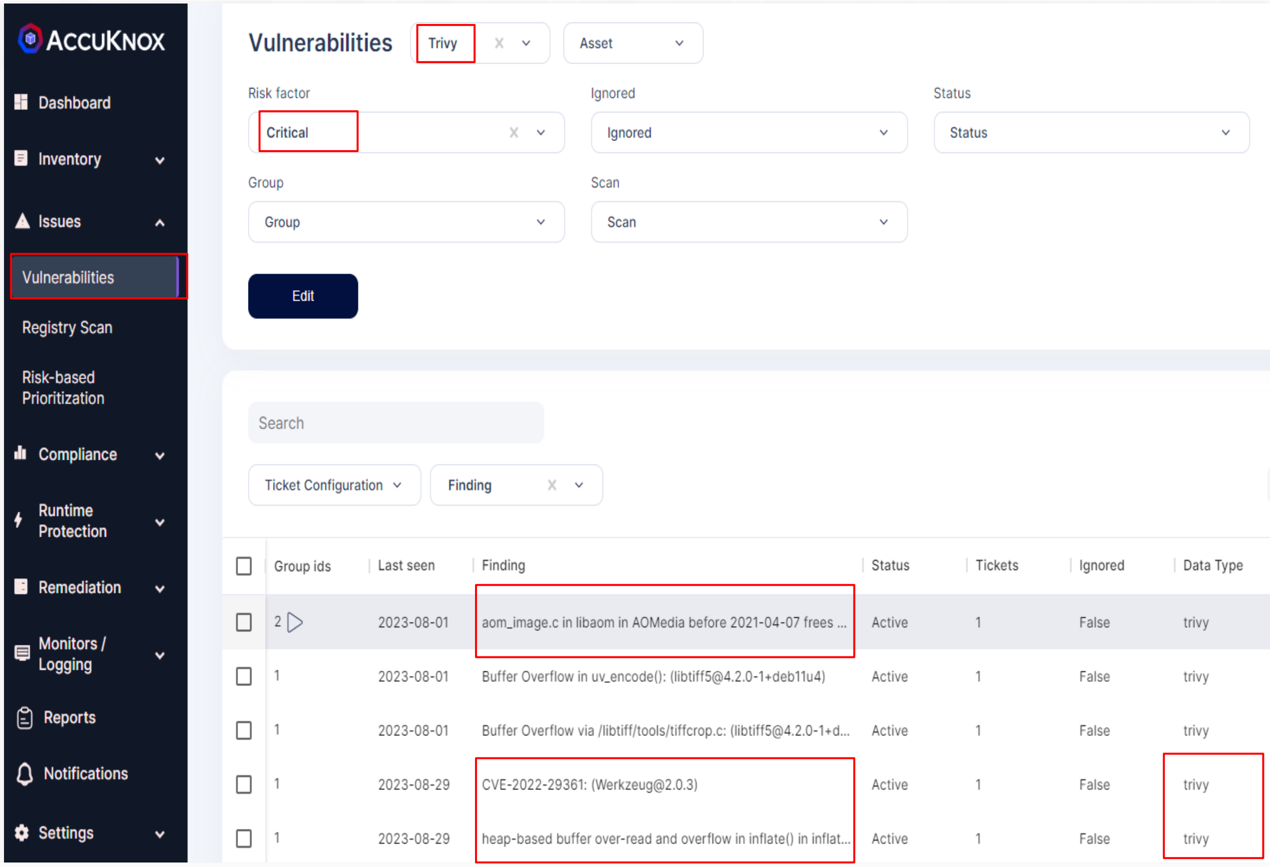
Beware

As the adage goes "an ounce of prevention is worth a pound of cure". Identifying basic and critical vulnerabilities in one's infrastructure is the first step in the cloud security journey.

Identify Container Images with Critical Vulnerabilities

To see the vulnerabilities associated with the Container Images, navigate to Issues → Vulnerabilities

- Apply **Trivy** in data-type filter
- Choose the severity “Critical” for the Findings



Vulnerabilities: Trivy | Asset

Risk factor: Critical

Ignored: Ignored

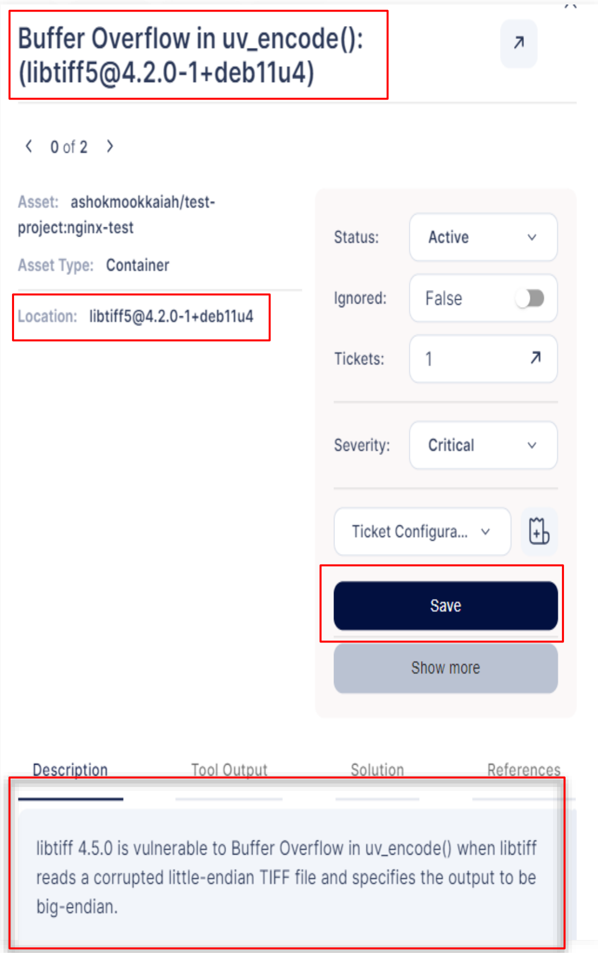
Status: Status

Group: Group

Scan: Scan

Ticket Configuration | Finding

	Group ids	Last seen	Finding	Status	Tickets	Ignored	Data Type
□	2 ▷	2023-08-01	aom_image.c in libaom in AOMedia before 2021-04-07 frees ...	Active	1	False	trivy
□	1	2023-08-01	Buffer Overflow in uv_encode(): (libtiff5@4.2.0-1+deb11u4)	Active	1	False	trivy
□	1	2023-08-01	Buffer Overflow via /libtiff/tools/tiffcrop.c: (libtiff5@4.2.0-1+d...	Active	1	False	trivy
□	1	2023-08-29	CVE-2022-29361: (Werkzeug@2.0.3)	Active	1	False	trivy
□	1	2023-08-29	heap-based buffer over-read and overflow in inflate() in inflat...	Active	1	False	trivy



Buffer Overflow in uv_encode(): (libtiff5@4.2.0-1+deb11u4)

Asset: ashokmookkaiah/test-project:nginx-test

Asset Type: Container

Location: libtiff5@4.2.0-1+deb11u4

Status: Active

Ignored: False

Tickets: 1

Severity: Critical

Ticket Configura...

libtiff 4.5.0 is vulnerable to Buffer Overflow in uv_encode() when libtiff reads a corrupted little-endian TIFF file and specifies the output to be big-endian.

Focus

Cloudsploit’s robust data-type filtering and granular search capabilities enable the easy identification of critical vulnerabilities. Streamlining security measures and protecting cloud infrastructure against potential risks is simple as it gets.

Shift Left – AccuKnox AppSec's Unified Approach

Problem: Noise

Most Vulnerabilities are **Noise** due to

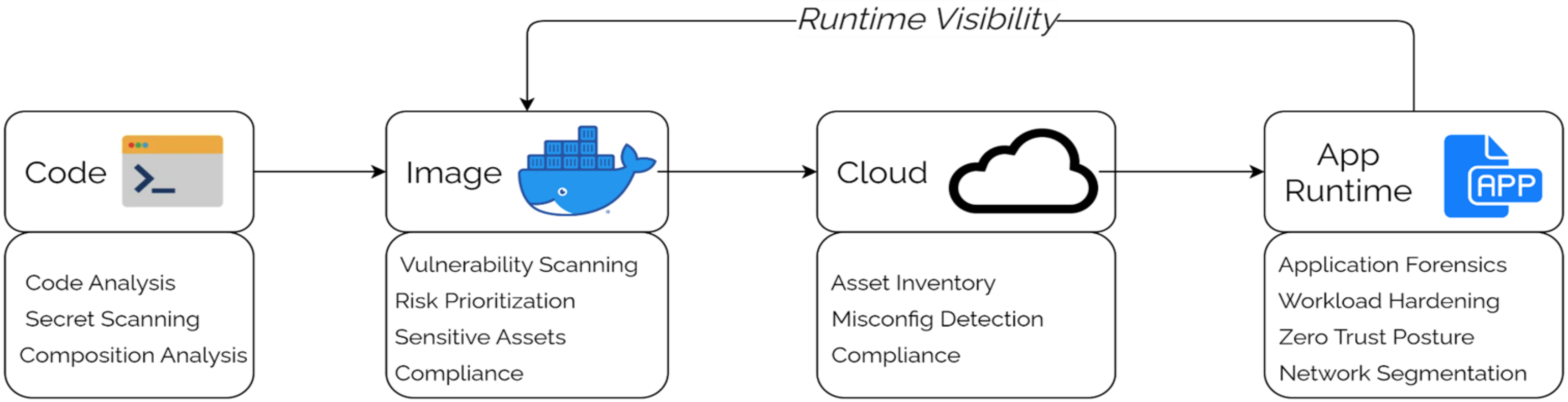
- False Positives
- Unexploitable
- Unused at Runtime
- **Too many** findings with no Runtime Context!!

AppSec and CloudSec works in silos and don't have contextual understanding of Vulnerabilities

Solution: AccuKnox AppSec

Revolutionizing Application Security

AccuKnox AppSec integrates best in class Vulnerability Management, SCA, SAST and DAST tools. Our flexible security posture approach efficiently prioritizes critical vulnerabilities, ensuring a comprehensive protection journey from code to cloud



Runtime Visibility

Code

Code Analysis
Secret Scanning
Composition Analysis

Image

Vulnerability Scanning
Risk Prioritization
Sensitive Assets
Compliance

Cloud

Asset Inventory
Misconfig Detection
Compliance

App Runtime

Application Forensics
Workload Hardening
Zero Trust Posture
Network Segmentation

Strategy

A critical part of Cloud Security journey is to integrate with AppSec (SAST, DAST, SCA) platforms. this ensures that any issues, vulnerabilities in the development phase is fully addressed during the deployment and run-time phases.

ASPM – Application Security Posture Management

SAST

Definition – analyzes source code for potential security vulnerabilities without running application

Used at – during development

Advantages – ability to fail a build in CI pipeline

Disadvantages – lots of false positives, runtime context

Cost – significant

Use-case:

- finding common CVE
- coding errors
- security best practices

Tools Supported

sonarqube FORTIFY

VERACODE

DAST or API Sec

Definition – simulate attack scenarios at running app to find vuln

Used at – post-development (test or production)

Advantages – identify vuln in running environment

Disadvantages – may miss some vuln, false positives, slow down app

Cost – significant

Use-case:

- finding common CVE
- coding errors
- security best practices

Tools Supported

OWASP Zed Attack Proxy Burp Suite

Tools WIP

VERACODE nuclei

WAS Qualys, Inc. Google TSUNAMI HCL AppSca

Key Takeaway

SAST analyzes source code during development, allowing failures in the CI pipeline. It is costly and prone to false positives. DAST simulates attack scenarios post-development, identifying vulnerabilities and aligning with AccuKnox's security offerings.

SAST

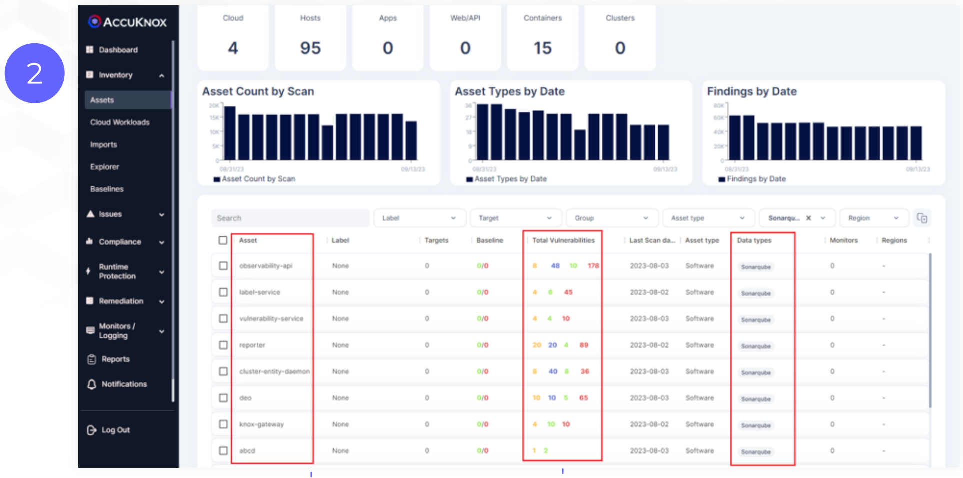
Integrate **Sonarqube** with your code repository through a JWT session-based token from AccuKnox SaaS

Step 1: Create workflow action for GitHub with token

Step 2: Workflow will be triggered for every PR raised

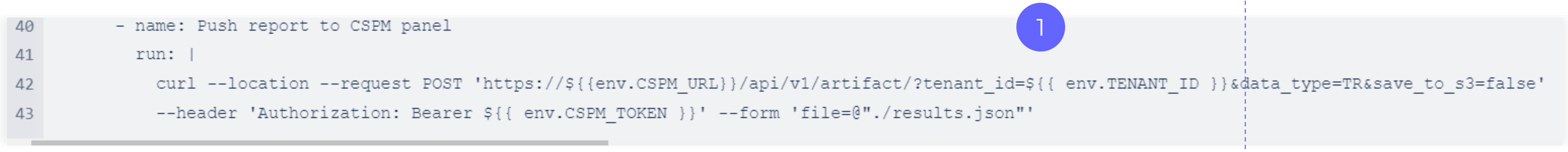
Step 3: Push result to AccuKnox SaaS

Filter Data Source as **Sonarqube** and it will help to identify all the coding errors, common CVE etc. associated with your repository



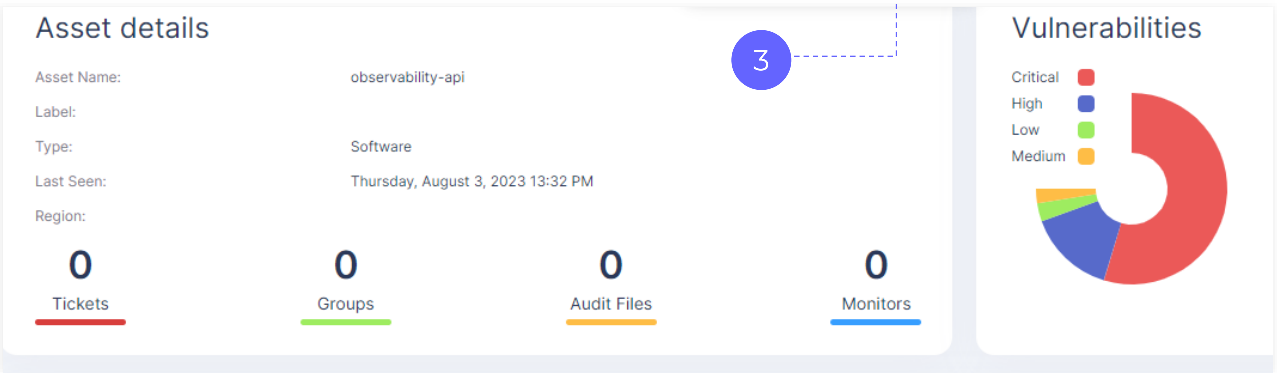
Cloud	Hosts	Apps	Web/API	Containers	Clusters
4	95	0	0	15	0

Asset	Label	Targets	Baseline	Total Vulnerabilities	Last Scan da...	Asset type	Data types	Monitors	Regions
observability-api	None	0	0/0	8 48 10 178	2023-08-03	Software	Sonarqube	0	-
label-service	None	0	0/0	4 6 45	2023-08-02	Software	Sonarqube	0	-
vulnerability-service	None	0	0/0	4 4 10	2023-08-03	Software	Sonarqube	0	-
reporter	None	0	0/0	20 20 4 89	2023-08-02	Software	Sonarqube	0	-
cluster-entity-daemon	None	0	0/0	8 40 8 36	2023-08-03	Software	Sonarqube	0	-
deo	None	0	0/0	10 10 5 65	2023-08-03	Software	Sonarqube	0	-
knox-gateway	None	0	0/0	4 10 10	2023-08-02	Software	Sonarqube	0	-
abcd	None	0	0/0	1 2	2023-08-03	Software	Sonarqube	0	-



```
      - name: Push report to CSPM panel
        run: |
          curl --location --request POST 'https://${{env.CSPM_URL}}/api/v1/artifact/?tenant_id=${{ env.TENANT_ID }}&data_type=TR&save_to_s3=false'
          --header 'Authorization: Bearer ${{ env.CSPM_TOKEN }}' --form 'file=@"./results.json"'
```

Get in touch with AccuKnox Team for assistance



Asset details

Asset Name: observability-api

Label:

Type: Software

Last Seen: Thursday, August 3, 2023 13:32 PM

Region:

Tickets	Groups	Audit Files	Monitors
0	0	0	0

Key Takeaway

Through a secure JWT token integration, AccuKnox and Sonarqube can analyze code automatically on GitHub pull requests. It finds common CVEs and coding errors for improved security and audit.

SCA

Definition –analyzes 3rd party dependencies/lib in open source

Used at – during dev, test or production

Advantages – identify vulnerable 3rd party sw

Disadvantages – no runtime context, limit 3rd party scope, does not scan code

Cost – less significant

Use-case:

- Identifying open-source component risks.
- Protecting against supply chain attacks. Checking dependencies for vulnerabilities.

Tools Supported

sonatype

aqua trivy

Tools WIP

VERACODE

BLACKDUCK BY SYNOPSYS

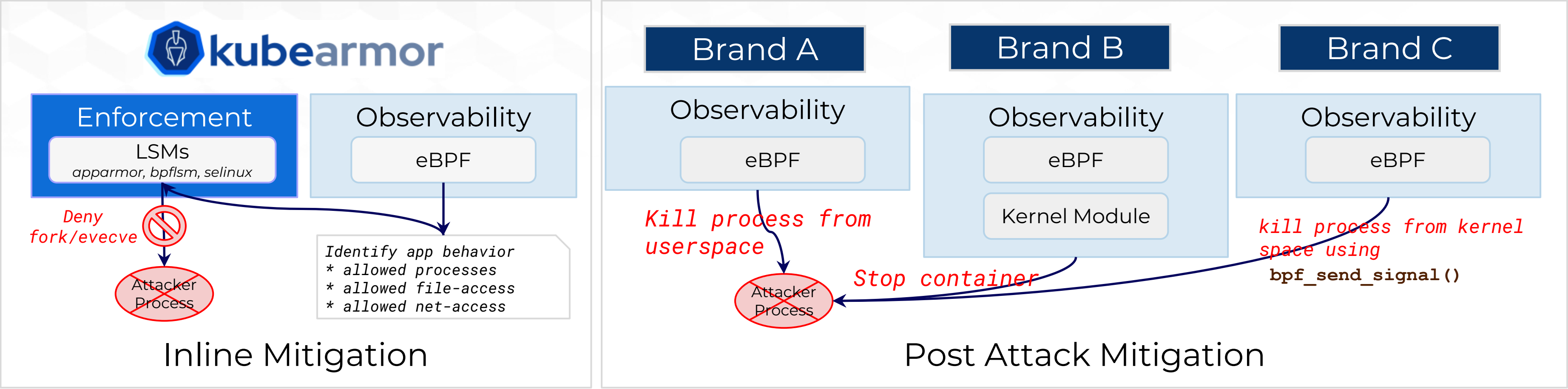
snyk

Type	Vulnerability	Severity	Runtime Visibility	Final Severity	Actions
Vulnerability	ncurses: segfaulting OOB read: (ncurses-terminfo-base@6.3_p20211120-ro)	7.1 (High)	ncurses module: Not used at runtime	Low	Virtual Patch Policy
Vulnerability	busybox: remote attackers may execute arbitrary code if netstat is used: (busybox@1.34.1-r3)	8.8 (High)	netstat module: In use at runtime	Critical	Upgrade busybox
Sensitive Asset	key.cert contains private key	Critical	key.cert: Not used at runtime	Low	Virtual Patch Policy
Sensitive Asset	root.pem contains sensitive key	Critical	root.pem is in use at runtime by /bin/vault process	High	Virtual Patch Policy

Key Takeaway

A secure software supply chain is ensured by AccuKnox's integration of Software Composition Analysis (SCA) into the development lifecycle. Simplified process to recognize and address vulnerabilities in open-source components.

KubeArmor's Distinctive Edge in Runtime Security Solutions


kubearmor

Enforcement

LSMs

apparmor, bpflsm, selinux

Observability

eBPF

Deny fork/evecve

Attacker Process

Identify app behavior
* allowed processes
* allowed file-access
* allowed net-access

Inline Mitigation

Brand A

Observability

eBPF

Kill process from userspace

Brand B

Observability

eBPF

Kernel Module

Stop container

Brand C

Observability

eBPF

kill process from kernel space using

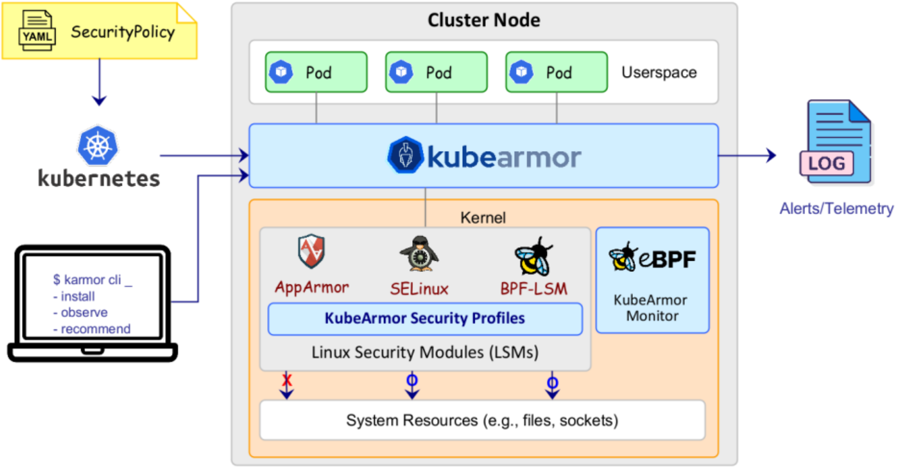
bpf_send_signal()

Attacker Process

Post Attack Mitigation

Differentiating Factors of KubeArmor:

- Restricts container behavior at the system level, covering process execution, file access, networking operations, and resource utilization.
- LSMs for security policies at runtime for each workload based on container or workload identities (e.g., labels).
- Generates logs for policy violations. eBPF-based monitoring to track container processes. Prompt alert on security policy breaches
- Simplifies policy management by handling internal complexities related to LSMs.
- Define and apply security policies based on metadata.


YAML SecurityPolicy

kubernetes

$ karmor cli _
- install
- observe
- recommend

Cluster Node

Pod

Pod

Pod

Userspace

kubearmor

Kernel

AppArmor

SELinux

BPF-LSM

KubeArmor Security Profiles

Linux Security Modules (LSMs)

eBPF

KubeArmor Monitor

System Resources (e.g., files, sockets)

LOG

Alerts/Telemetry

Key Takeaway

AccuKnox is powered by KubeArmor Discovery Engine. It simplifies policy management for effective, metadata-driven security solutions. Granular security policies are enforced at the system level with real-time monitoring for prompt alerts.

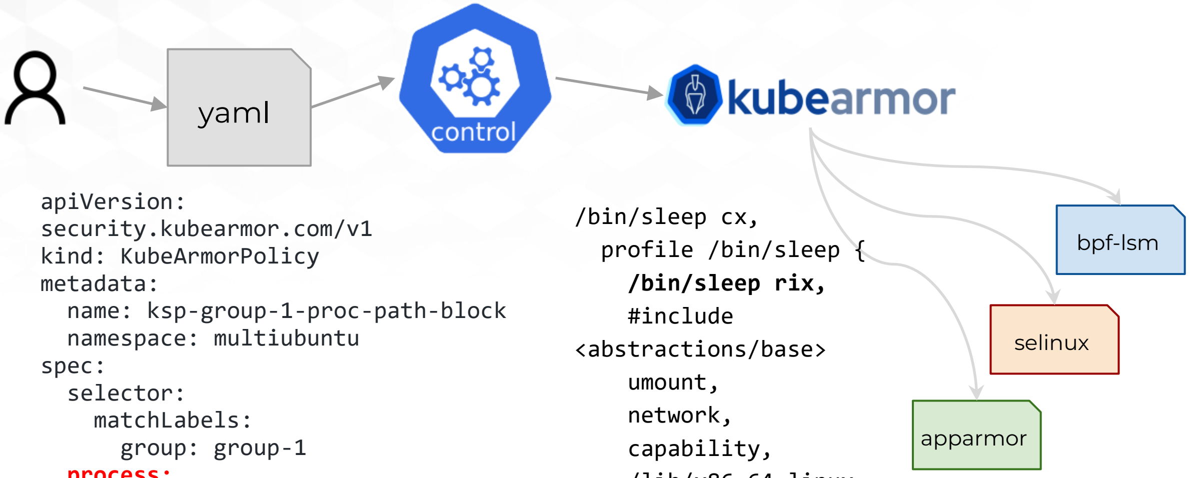
KubeArmor Enforcement Differentiation

Runtime Security Engine

Preventing Actions/Attacks

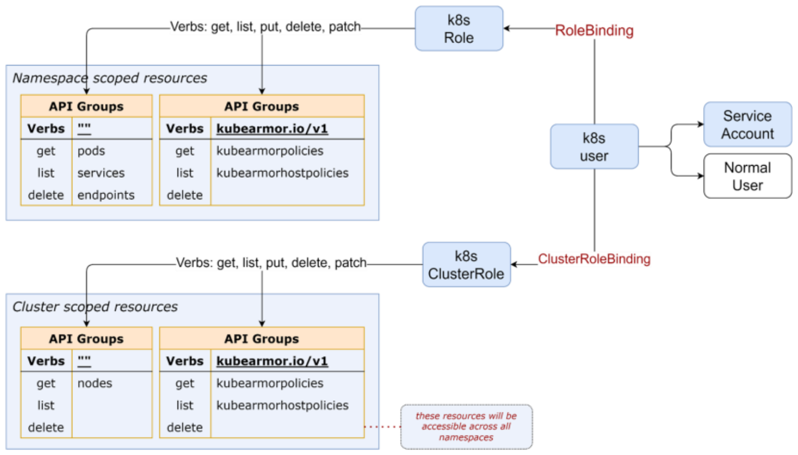
Deployment Modes

- K8s as DaemonSet
- Pure Containerized Mode
- Systems Mode



```
apiVersion:
security.kubearmor.com/v1
kind: KubeArmorPolicy
metadata:
  name: ksp-group-1-proc-path-block
  namespace: multiubuntu
spec:
  selector:
    matchLabels:
      group: group-1
  process:
    matchPaths:
    - path: /bin/sleep
  action:
      Block
```

```
/bin/sleep cx,
  profile /bin/sleep {
    /bin/sleep rix,
    #include
<abstractions/base>
    umount,
    network,
    capability,
    /lib/x86_64-linux-
gnu/{*,**} rm,
    /lib/{*,**} rm,
    /lib/modules/{*,**}
rm,
```



Namespace scoped resources

API Groups	
Verbs	""
get	pods
list	services
delete	endpoints

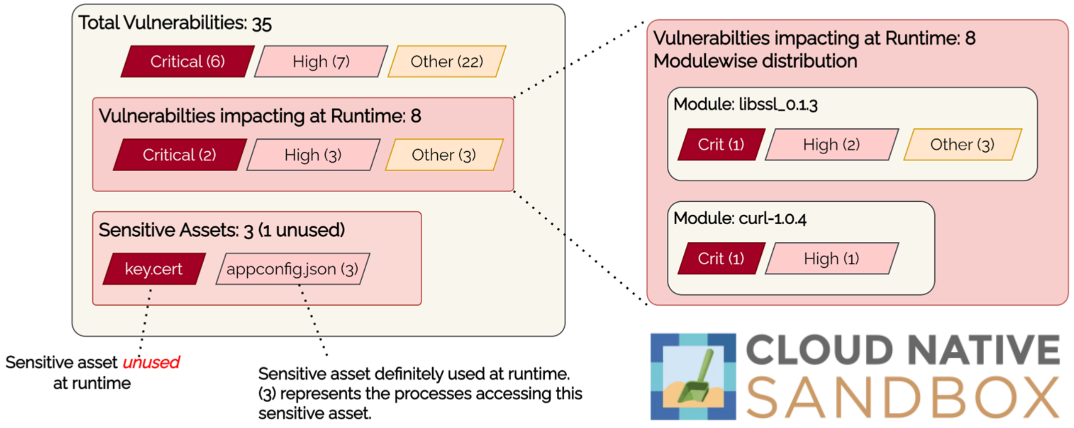
API Groups	
Verbs	kubearmor.io/v1
get	kubearmorpolicies
list	kubearmorhostpolicies
delete	

Cluster scoped resources

API Groups	
Verbs	""
get	nodes
list	
delete	

API Groups	
Verbs	kubearmor.io/v1
get	kubearmorpolicies
list	kubearmorhostpolicies
delete	

these resources will be accessible across all namespaces


Total Vulnerabilities: 35
Critical (6)
High (7)
Other (22)
Vulnerabilties impacting at Runtime: 8
Critical (2)
High (3)
Other (3)
Sensitive Assets: 3 (1 unused)
key.cert
appconfig.json (3)
Vulnerabilties impacting at Runtime: 8
Modulewise distribution
Module: libssl_0.1.3
Crit (1)
High (2)
Other (3)
Module: curl-1.0.4
Crit (1)
High (1)
Sensitive asset unused at runtime
Sensitive asset definitely used at runtime. (3) represents the processes accessing this sensitive asset.

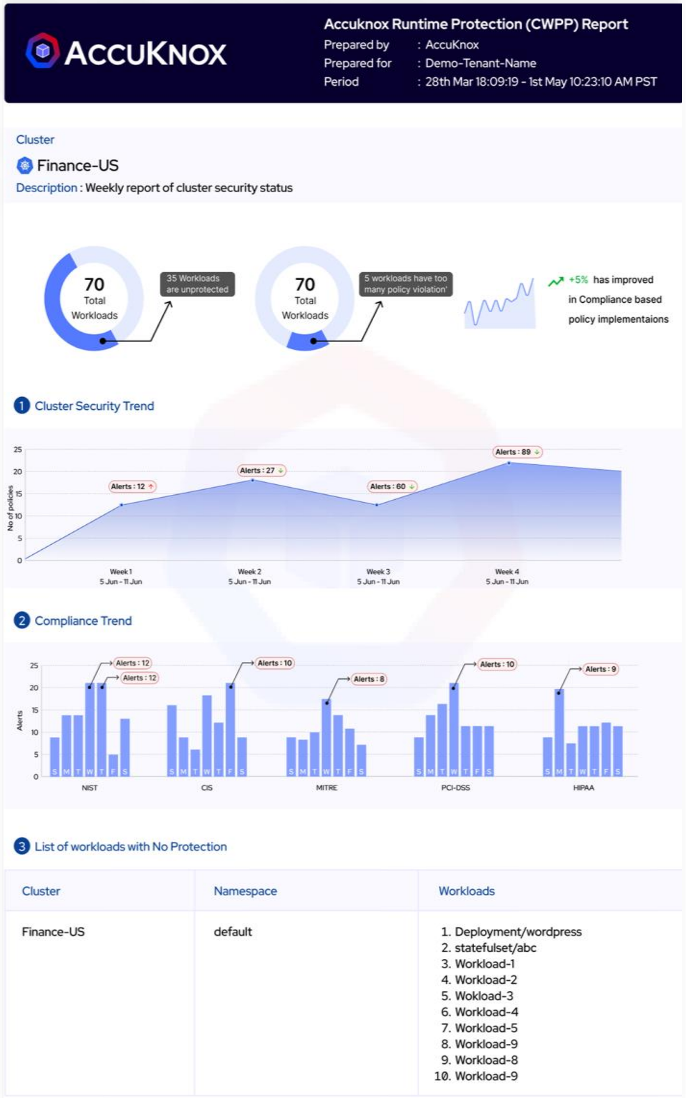
CLOUD NATIVE SANDBOX

Technical Stuff

KubeArmor generates human readable policies and is in keeping with modern practices “security as code”, “policy as code”. As a CNCF Open Source project it is being adopted by thousands of organizations globally.

CWPP – Cloud Workload Protection Platform

Type	Vulnerability
Zero Trust	Auto Discovered Zero Trust Policy
	Custom Zero Trust Policy
	Inline Remediation
	Network Microsegmentation
Recommendations	Workload Hardening Policies
Monitoring	Logs and Alerts
Orchestration	Multi User, Multi Tenant, Multi Cluster Management
Integrations	Channel Integrations
Deployments	k8s workloads support
	VM and Bare-Metal support
Compliance	File Integrity Monitoring
	Continuous Compliance
Roadmap	Admission Controller Support
	KIEM (K8s Identities & Entitlements Management)
	Fargate Support



ACCUKNOX

Accuknox Runtime Protection (CWPP) Report

Prepared by : AccuKnox
Prepared for : Demo-Tenant-Name
Period : 28th Mar 18:09:19 - 1st May 10:23:10 AM PST

Cluster

Finance-US

Description : Weekly report of cluster security status

70
Total
Workloads
35 Workloads are unprotected
70
Total
Workloads
5 workloads have too many policy violation'
+5% has improved in Compliance based policy implementaions

1 Cluster Security Trend

2 Compliance Trend

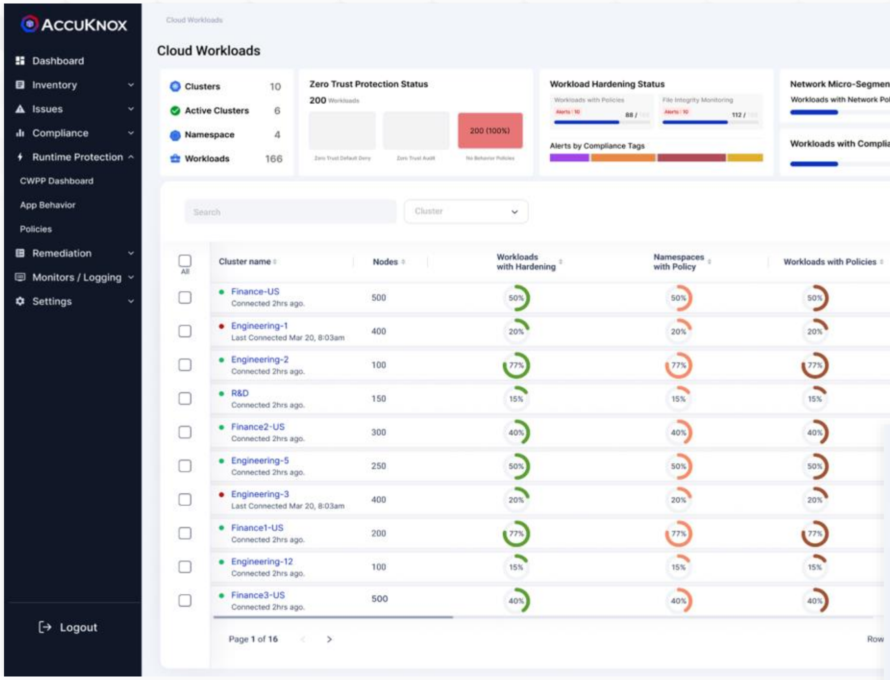
3 List of workloads with No Protection

Cluster	Namespace	Workloads
Finance-US	default	1. Deployment/wordpress 2. statefulset/abc 3. Workload-1 4. Workload-2 5. Wokload-3 6. Workload-4 7. Workload-5 8. Workload-9 9. Workload-8 10. Workload-9

Strategy

CWPP – Cloud Workload Protection Platform allows one to adopt the well-known approach of "Defense in Depth". While CSPM delivers functionality to address static security issues, CWPP helps one address Zero Day attacks, run-time attacks.

CWPP – Fortifying Applications, Enforcing Zero Trust, Ensuring Security Resilience



Cloud Workloads

Clusters	10
Active Clusters	6
Namespace	4
Workloads	166

Zero Trust Protection Status: 200 Workloads; 200 (100%) No Behavior Policies

Workload Hardening Status: Workloads with Policies, Alerts : 10, 88 /; File Integrity Monitoring, Alerts : 10, 112 /

Alerts by Compliance Tags

Network Micro-Segmentation: Workloads with Network Policies 12 /

Workloads with Compliance Policies 12 /

Cluster name	Nodes	Workloads with Hardening	Namespaces with Policy	Workloads with Policies	Alerts
Finance-US Connected 2hrs ago.	500	50%	50%	50%	5
Engineering-1 Last Connected Mar 20, 8:03am	400	20%	20%	20%	10
Engineering-2 Connected 2hrs ago.	100	77%	77%	77%	15
R&D Connected 2hrs ago.	150	15%	15%	15%	12
Finance2-US Connected 2hrs ago.	300	40%	40%	40%	
Engineering-5 Connected 2hrs ago.	250	50%	50%	50%	
Engineering-3 Last Connected Mar 20, 8:03am	400	20%	20%	20%	
Finance1-US Connected 2hrs ago.	200	77%	77%	77%	
Engineering-12 Connected 2hrs ago.	100	15%	15%	15%	
Finance3-US Connected 2hrs ago.	500	40%	40%	40%	

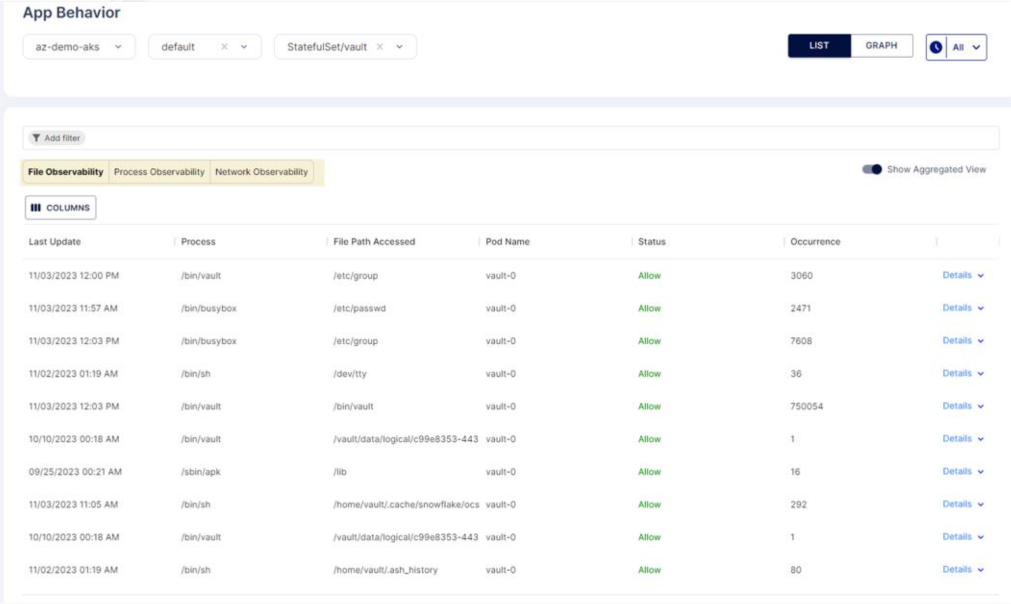
Page 1 of 16

Application Security

1. Posture Discovery
2. Behavior Analysis
3. Remote Code Exec Protection
4. Cryptocurrency-mining Prevention
5. File Integrity Monitoring

Zero Trust Hardening

1. HashiCorp Vault
2. CyberArk Conjur



Last Update	Process	File Path Accessed	Pod Name	Status	Occurrence	
11/03/2023 12:00 PM	/bin/vault	/etc/group	vault-0	Allow	3060	Details
11/03/2023 11:57 AM	/bin/busybox	/etc/passwd	vault-0	Allow	2471	Details
11/03/2023 12:03 PM	/bin/busybox	/etc/group	vault-0	Allow	7608	Details
11/02/2023 01:19 AM	/bin/sh	/dev/tty	vault-0	Allow	36	Details
11/03/2023 12:03 PM	/bin/vault	/bin/vault	vault-0	Allow	750054	Details
10/10/2023 00:18 AM	/bin/vault	/vault/data/logical/c99e8353-443	vault-0	Allow	1	Details
09/25/2023 00:21 AM	/sbin/apk	/lib	vault-0	Allow	16	Details
11/03/2023 11:05 AM	/bin/sh	/home/vault/.cache/snowflake/ocs	vault-0	Allow	292	Details
10/10/2023 00:18 AM	/bin/vault	/vault/data/logical/c99e8353-443	vault-0	Allow	1	Details
11/02/2023 01:19 AM	/bin/sh	/home/vault/.ash_history	vault-0	Allow	80	Details

Security Measures

1. Man-in-the-Middle Attack Prevention
2. Denial-of-Service Protection

User Security

1. Covering Tracks Prevention
2. Impersonation Defense
3. Privilege Escalation Protection

Technical Stuff

CWPP helps one address Zero Day attacks, run-time attacks by delivering critical Zero Trust security capabilities like (1) Micro-segmentation (2) Application Firewalling (3) Kernel Hardening.

Agent or Agentless – YES is the answer!

Agentless **CSPM** (Cloud Security Posture Management)	**Basic Security**	**Multi-Cloud Security and Compliance** Posture Discovery, and protection through the use of native APIs
	Application Security	App Security from **Code to Run**
Lightweight Industry Standard (eBPF) Sensor Agent **CWPP** Cloud Workload Protection Platform	**Container Forensics and Auditing**	**eBPF** (Extended Berkeley Packet Filter) based Observability with **Auto-Discovery of App Behavior** at process-level granularity
	Workload Hardening, Zero Trust Security	Comply with NSA Kubernetes Hardening Guide. **- Application Firewalling** **- Micro-segmentation** **- Kernel Hardening** to defend against zero-day attacks. Use eBPF for observability and LSMs (Linux Security Modules) to move from observability (audit) to enforcement (block) mode

Brilliant Idea AccuKnox CNAPP delivers immense functionality without requiring an agent and provides advanced run-time functionality using an industry standard agent.

Beware of solutions that require proprietary agents, kernel modifications, etc.

Defense in-Depth – Multi Layer Zero Trust Security

Q. Why Multi Layer Zero Trust?
A. Zero Trust philosophy at every level

Application

- Least permissive access to secrets and data
- Fine grain monitoring and Application Hardening
- Application Isolation and containing blast radius

Transport

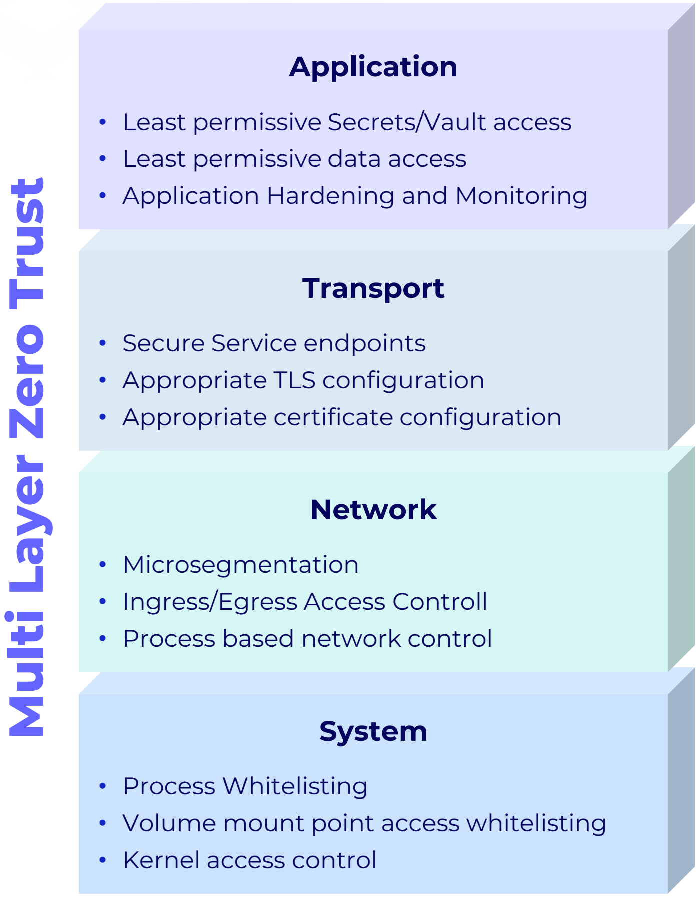
- Use of secure endpoints
- Ensure proper TLS and cert configuration

Network

- Micro-segmentation and Ingress/Egress control
- Process based Network access whitelisting

Systems

- Process Whitelisting
- Volume mount point access whitelisting
- Kernel security sensitive access primitives whitelisting



Multi Layer Zero Trust

Application

- Least permissive Secrets/Vault access
- Least permissive data access
- Application Hardening and Monitoring

Transport

- Secure Service endpoints
- Appropriate TLS configuration
- Appropriate certificate configuration

Network

- Microsegmentation
- Ingress/Egress Access Controll
- Process based network control

System

- Process Whitelisting
- Volume mount point access whitelisting
- Kernel access control

Focus

There were 70% more data breaches in 2022's Q3 than in Q2. Embrace Multi-Layer Zero Trust for robust security. From least permissive access at the application level to kernel-level whitelisting, fortify each layer to ensure comprehensive protection against evolving threats.

Zero Trust Synergy – Delivering Solutions At Every Stage

Elements of Zero Trust	AccuKnox Solution
Application Monitoring and Observability	KubeArmor: eBPF based monitoring
Application Hardening (NIST, MITRE, CIS, ENISA, FiGHT)	KubeArmor: eBPF + BPFLSM based enforcement
Network Microsegmentation	Discovery Engine + KubeArmor
Least permissive policies	Discovery Engine + KubeArmor
Process Whitelisting/Control	Discovery Engine + KubeArmor
Secure Endpoints	K8TLS
Service Mesh	K8tls + Existing Service Mesh [Roadmap]
CI/CD DevSecOps	GH Actions + KubeArmor + Discovery Engine
CIEM/KIEM (Identities and Entitlements)	AccuKnox Enterprise [coming soon]

Key Takeaway

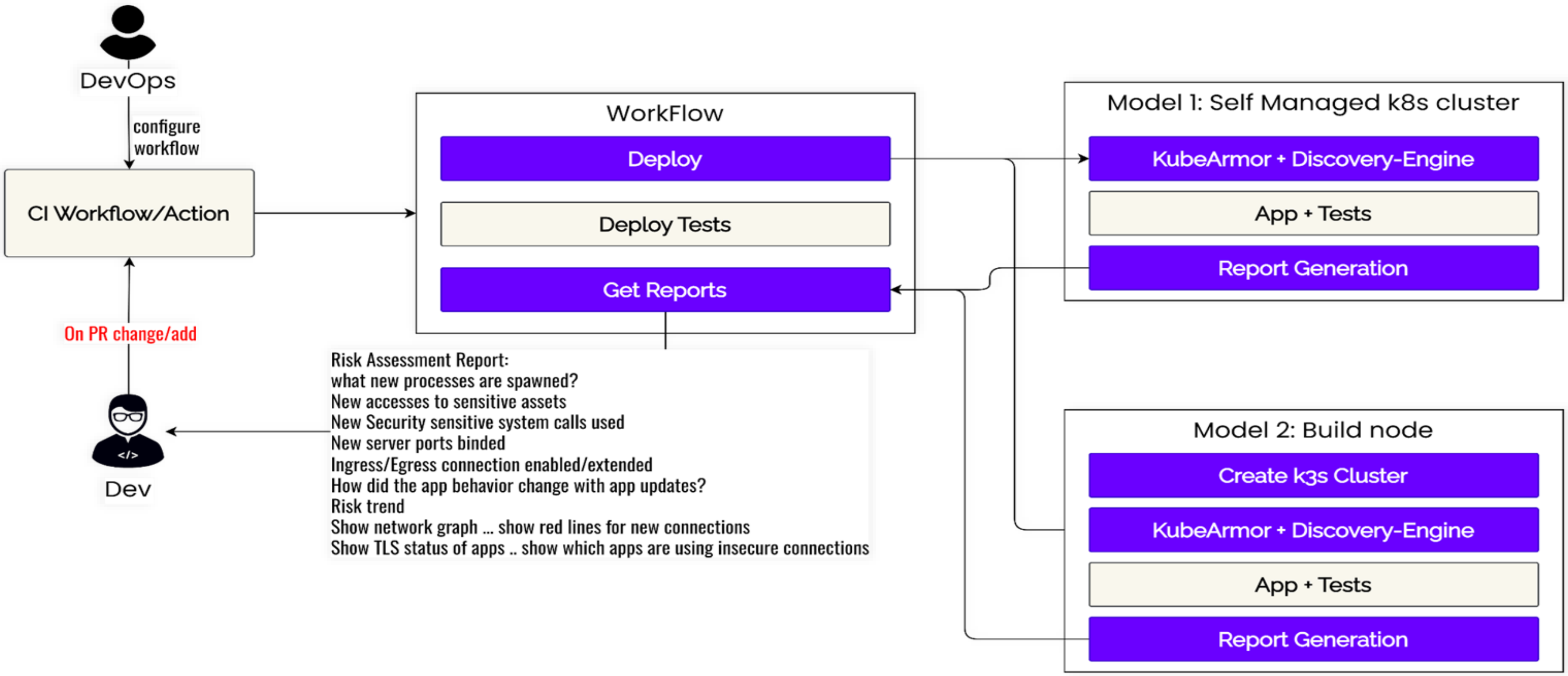
AccuKnox uses a Zero Trust framework with KubeArmor, NIST, MITRE, CIS, ENISA, FiGHT-compliant Application Hardening, and Network Microsegmentation for enhanced security in development lifecycle.

Zero Trust Assurance and Simplified DevOps Workflow

Challenges with maintaining Zero Trust Security Posture

- Applications change over time
- Application Dependencies change over time
- Cloud configuration changes over time

AccuKnox tooling helps identify deviations in Zero Trust Posture early in dev lifecycle.



DevOps

configure workflow

CI Workflow/Action

On PR change/add

Dev

WorkFlow

Deploy

Deploy Tests

Get Reports

Model 1: Self Managed k8s cluster

KubeArmor + Discovery-Engine

App + Tests

Report Generation

Model 2: Build node

Create k3s Cluster

KubeArmor + Discovery-Engine

App + Tests

Report Generation

Risk Assessment Report:
what new processes are spawned?
New accesses to sensitive assets
New Security sensitive system calls used
New server ports binded
Ingress/Egress connection enabled/extended
How did the app behavior change with app updates?
Risk trend
Show network graph ... show red lines for new connections
Show TLS status of apps .. show which apps are using insecure connections

Key Takeaway

Our Zero Trust CNAPP integrates with DevOps workflows, providing continuous verification across applications and cloud configurations. Get dynamic security and a commitment to Zero Trust principles.

GRC – Governance Compliance and Risk

Empowering Secure Cloud Governance, Risk, Compliance

GRC
Governance, Risk management, and Compliance

SLOW paced, **PROCESS** driven, **POINT** in time

✓ Real-Time Adaptive Monitoring

MANUAL process of Compliance

✓ Continuous and Automated Compliance

SILOED and **FRAGMENTED** approach to GRC

✓ Integrated, Correlated and Connected

TRIAGE of Alerts dilute the focus into high severity issues

✓ Proactive Remediation and Zero False Positives

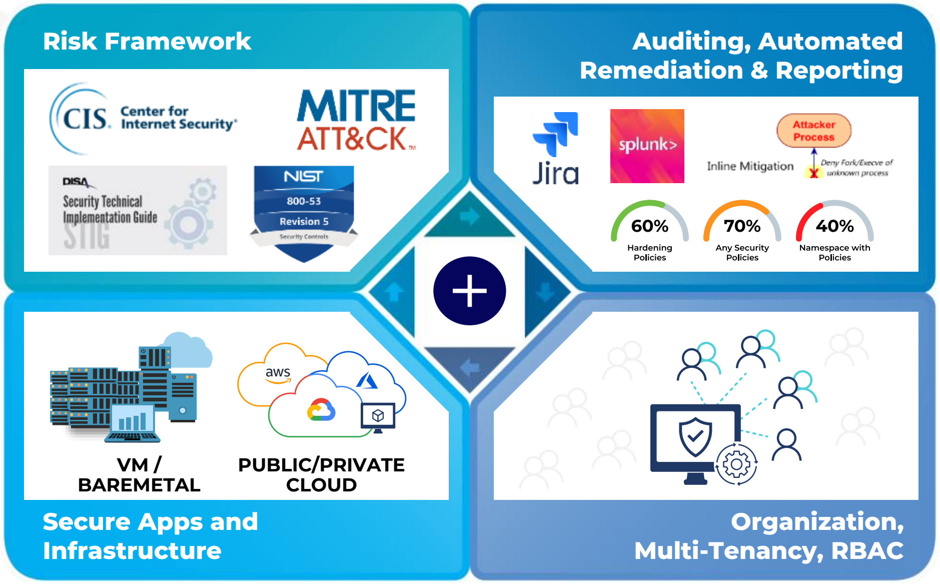
COMPLEX environment having Multi-Tenant, Multi-Cloud and RBAC control

✓ Multi-Cloud, Hybrid-Cloud and On-Prem

Key Takeaway

AccuKnox uses strong governance, multi-tenancy, RBAC controls, duty separation, thorough risk assessment, automation, and compliance standards to provide a safe, legal, and auditable cloud infrastructure.

AccuKnox GRC Approach



Risk Framework

Auditing, Automated Remediation & Reporting

Secure Apps and Infrastructure

Organization, Multi-Tenancy, RBAC

CIS. Center for Internet Security
MITRE ATT&CK
DISA Security Technical Implementation Guide STIG
NIST 800-53 Revision 5 Security Controls
Jira
splunk>
Inline Mitigation
Attacker Process
Deny Fork/Execve of unknown process
60% Hardening Policies
70% Any Security Policies
40% Namespace with Policies
+
VM / BAREMETAL
aws
PUBLIC/PRIVATE CLOUD

GRC ROADMAP

- Onboarding
- Auto-Discover Posture
- Baseline
- Continuous Observability
- Mode of Enforcement
- Reporting, Analytics and Auditing

Comprehensive and Automated GRC Platform

- Enforce Risk Framework conformance
- Visibility across entire infra or app
- Manage Organization multi-tenancy, RBAC
- Real-time Monitoring and Auditing
- Proactive and Automated Remediation
- Comprehensive Reporting

1 GOVERNANCE

- Multi-Tenancy, RBAC controls, Separation of Duties
- Dashboard for definitions and runtime monitoring
- Continuous Logging, Monitoring, Alert and Audit
- Integrates into existing SOCs

2 RISK

- Auto-detect Security Posture for specific applications
- Automated generation of baseline and policy control
- Risk / compliance- based prioritization of the issues
- Workflow automation, monitoring , alerting, blocking on violation,
- Automated audit logs

3 COMPLIANCE

- System and application compliance with CIS1, CIS2, HIPAA, PCI-DSS, MITRE, NIST
- On demand Compliance Report
- Continuous, Periodic and On-demand scan
- Audit / Block based Remediation for violation
- Forensics, Audit Trail and RCA

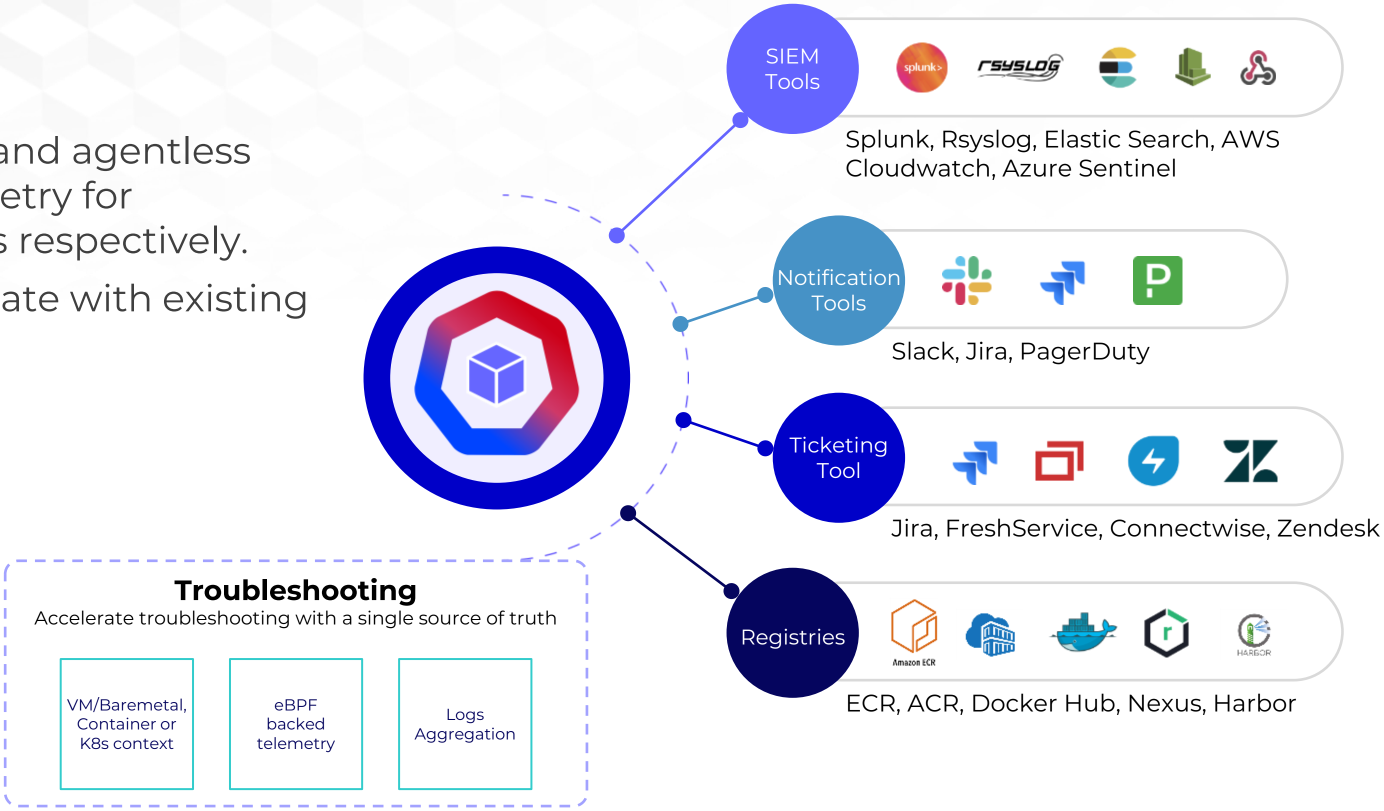
Integrations

- Our lightweight agent and agentless provides us deep telemetry for workload and resources respectively.
- It can seamlessly integrate with existing security and IT-tool

✓ Monitors

✓ Logging

✓ eBPF based Telemetry



SIEM Tools

Splunk, Rsyslog, Elastic Search, AWS Cloudwatch, Azure Sentinel

Notification Tools

Slack, Jira, PagerDuty

Ticketing Tool

Jira, FreshService, Connectwise, Zendesk

Registries

ECR, ACR, Docker Hub, Nexus, Harbor

Troubleshooting

Accelerate troubleshooting with a single source of truth

VM/Baremetal, Container or K8s context

eBPF backed telemetry

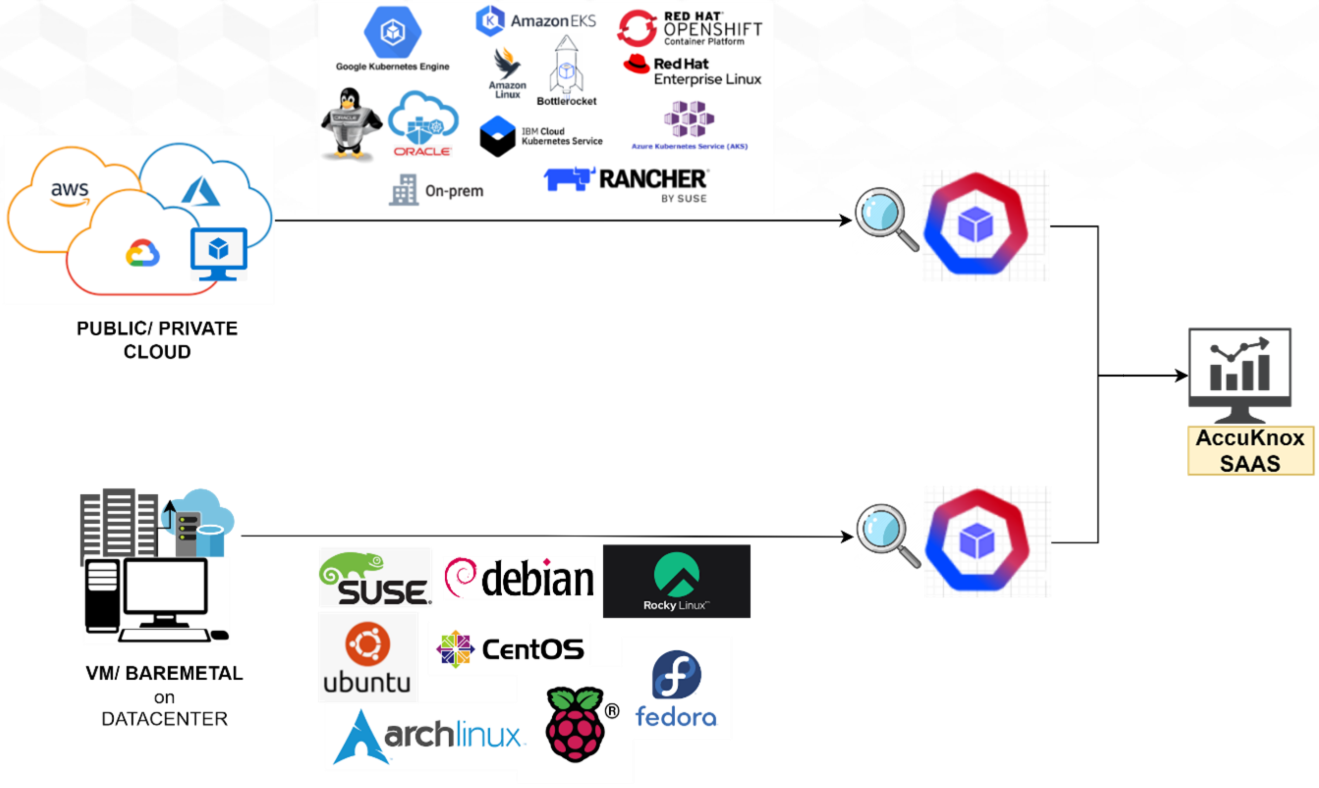
Logs Aggregation

Key Takeaway

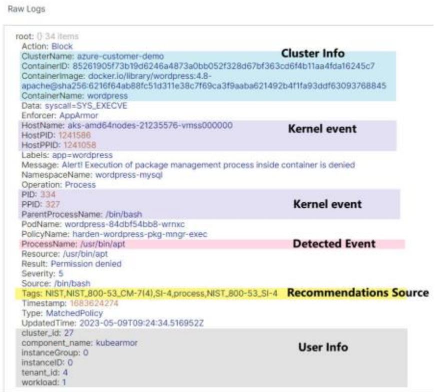
AccuKnox provides AccuKnox can integrate multiple Cloud Account, Registries, SIEM platform, Ticketing or Notifications Tools and the list is ever growing.

1. **Security Events/SIEM** : Splunk, Rsyslog, AWS CloudWatch, Elastic Search, Webhooks
2. **Notification Tools:** Slack, Jira, PagerDuty, Emails
3. **Ticketing Tools:** Jira, FreshService, Connectwise, Zendesk,
4. **Registries:** Nexus, ECR, GCR, DockerHub

Forensics



- eBPF powered rich **Telemetry**
  - **File** Accessed Logs
  - **Network** Connections Logs
  - **Process** Executed Logs
- **Audit** based Alerts
- **Block** based Alerts
- **Drift Detection** and Alerts



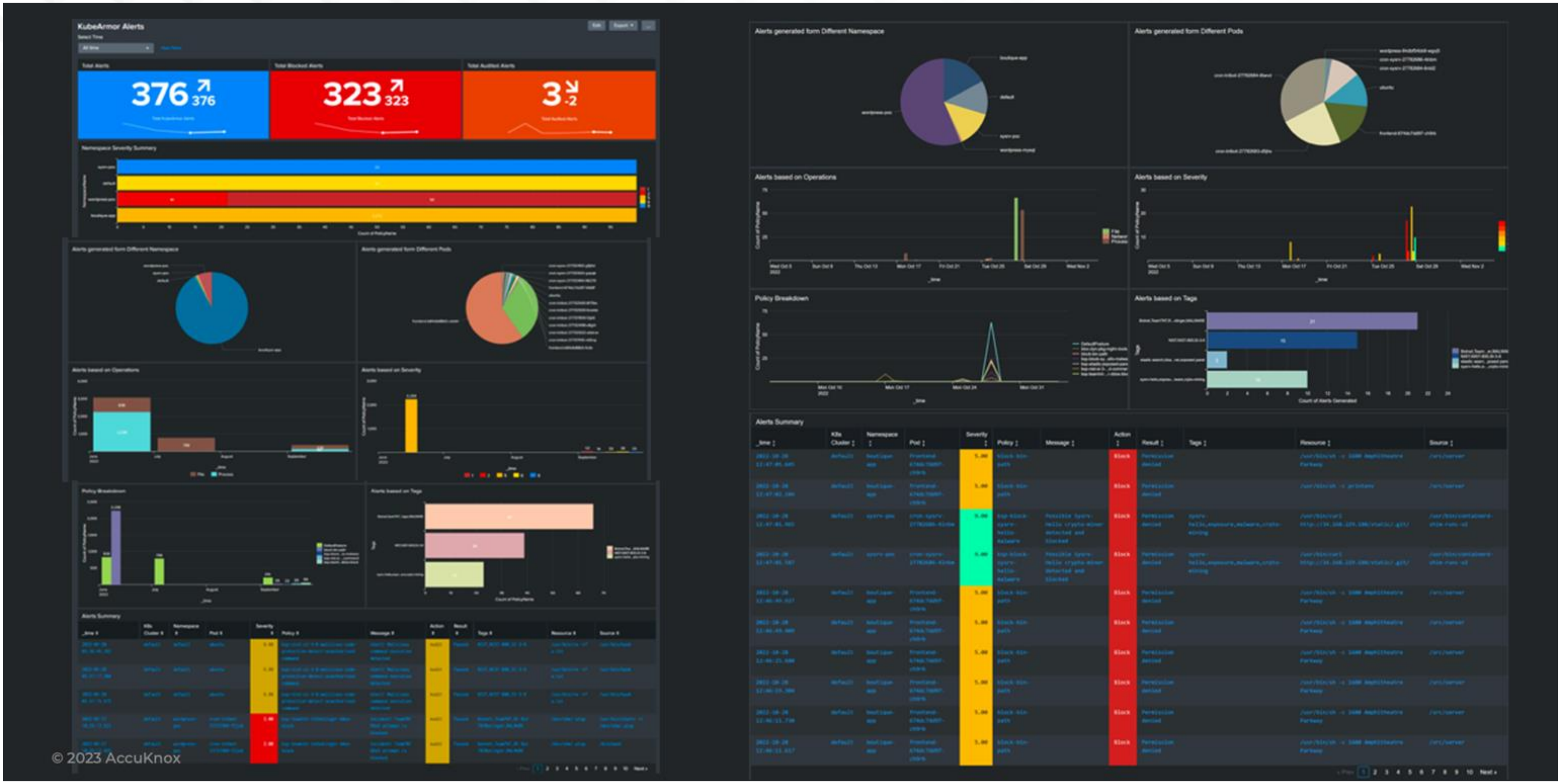
Raw Logs

```
root: {} 34 items
  Action: Block
  ClusterName: azure-customer-demo
  ContainerID: 85261905f73b19d6246a4873a0bb052f328d67bf363cd6f4b11aa4fda16245c7
  ContainerImage: docker.io/library/wordpress:4.8-
  apache@sha256:6216f64ab88fc51d311e38c7f69ca3f9aaba621492b4f1fa93ddf63093768845
  ContainerName: wordpress
  Data: syscall=SYS_EXECVE
  Enforcer: AppArmor
  HostName: aks-amd64nodes-21235576-vmss000000
  HostPID: 1241586
  HostPPID: 1241058
  Labels: app=wordpress
  Message: Alert! Execution of package management process inside container is denied
  NamespaceName: wordpress-mysql
  Operation: Process
  PID: 334
  PPID: 327
  ParentProcessName: /bin/bash
  PodName: wordpress-84dbf54bb8-wrnxc
  PolicyName: harden-wordpress-pkg-mngr-exec
  ProcessName: /usr/bin/apt
  Resource: /usr/bin/apt
  Result: Permission denied
  Severity: 5
  Source: /bin/bash
  Tags: NIST,NIST_800-53_CM-7(4),SI-4,process,NIST_800-53_SI-4
  Timestamp: 1683624274
  Type: MatchedPolicy
  UpdatedTime: 2023-05-09T09:24:34.516952Z
  cluster_id: 27
  component_name: kubearmor
  instanceGroup: 0
  instanceID: 0
  tenant_id: 4
  workload: 1
```

Key Takeaway

- AccuKnox delivers a complete package of forensics services (process information, file access information, network activity, security-sensitive system calls, and in-depth audits of sensitive asset accesses).
- These features cover virtual machines (VMs), public and private clouds, and on-premises installations.
- Get end-to-end insights for reliable security analysis, guaranteeing visibility and traceability across various computing environments.

SIEM Integration



Key Takeaway

AccuKnox integrates with popular SIEMs like Splunk, Elastic, Grafana, etc. to deliver telemetry and insights so that the SIEM can be used for Analysis, Forensics, Incident Response, Reporting, etc.

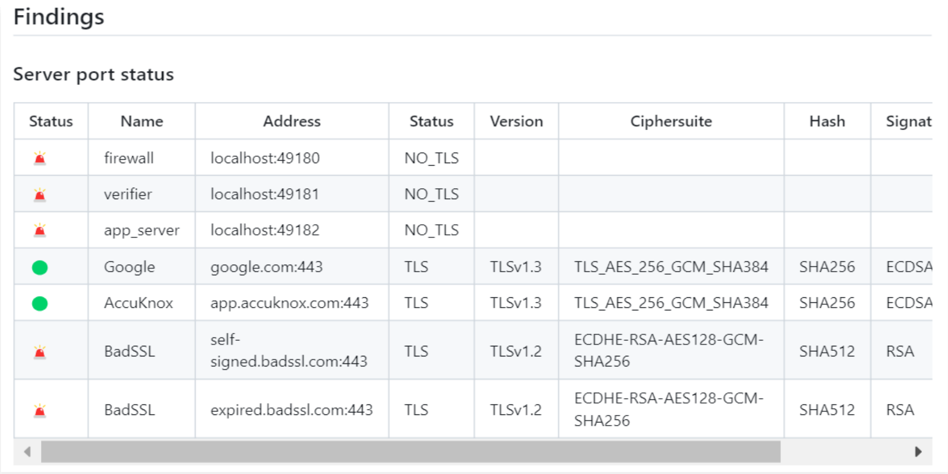
AccuKnox DevSecOps Techstack

- Harness potential of multiple open source tools and optionally commercial security scanner tools to provide early detection and remediation of vulnerabilities in a shift-left approach.
- Aggregate and normalize results from different sources as a SOAR platform

Relevant for – CI/CD Security, Infrastructure Misconfiguration, Compliance, Drift Detection and Benchmarking

CI/CD Pipeline

Commit To Repo	Build	Deploy
IDE Plugins	SAST	DAST
	SCA	IAST
		Container Vulnerabilities
		Registry/Image Scan
		API Sec
		Infrastructure as Code



Findings

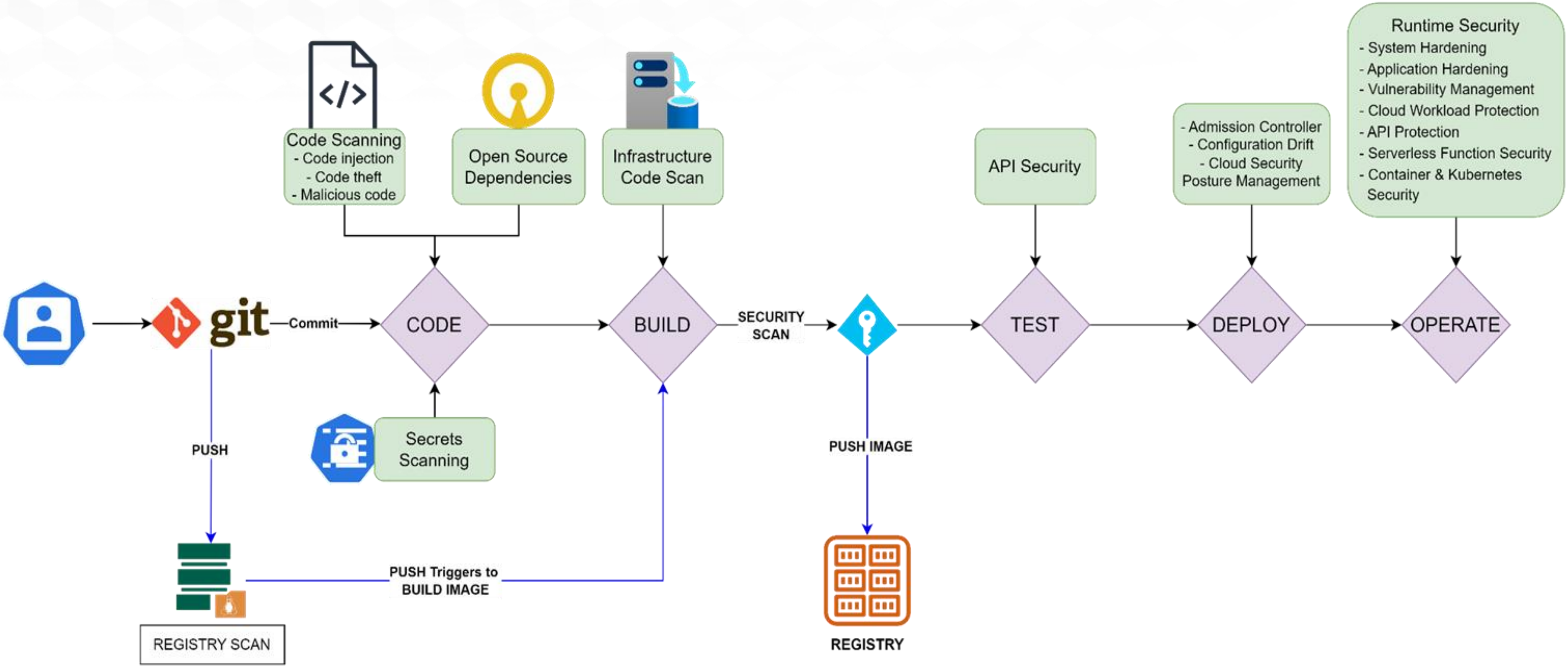
Server port status

Status	Name	Address	Status	Version	Ciphersuite	Hash	Signat
🚨	firewall	localhost:49180	NO_TLS				
🚨	verifier	localhost:49181	NO_TLS				
🚨	app_server	localhost:49182	NO_TLS				
●	Google	google.com:443	TLS	TLSv1.3	TLS_AES_256_GCM_SHA384	SHA256	ECDSA
●	AccuKnox	app.accuknox.com:443	TLS	TLSv1.3	TLS_AES_256_GCM_SHA384	SHA256	ECDSA
🚨	BadSSL	self-signed.badssl.com:443	TLS	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256	SHA512	RSA
🚨	BadSSL	expired.badssl.com:443	TLS	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256	SHA512	RSA

Key Takeaway

AccuKnox uses strong governance, multi-tenancy, RBAC controls, duty separation, thorough risk assessment, automation, and compliance standards to provide a safe, legal, and auditable cloud infrastructure.

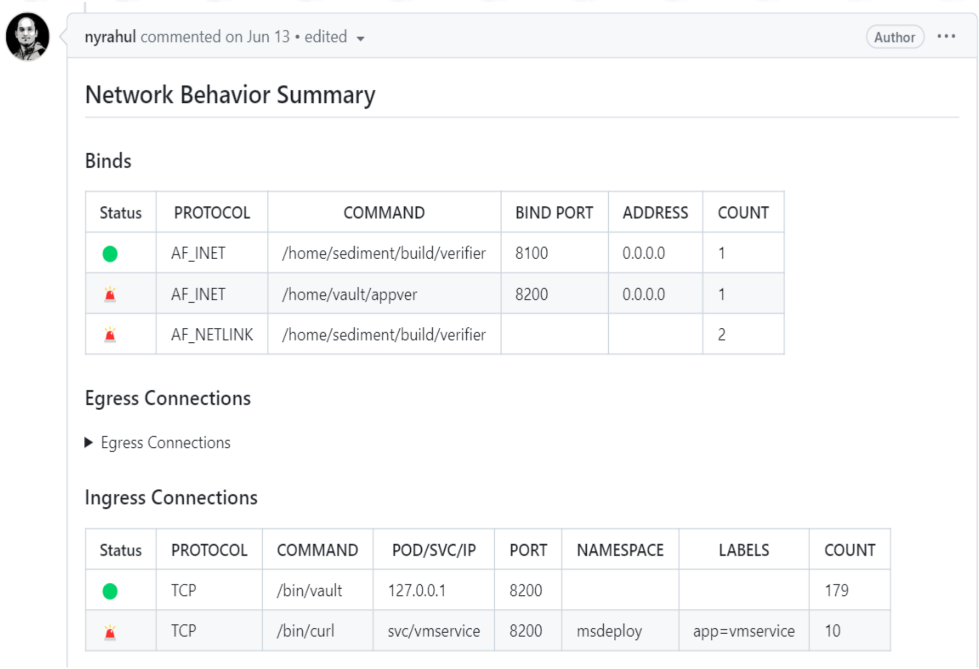
Orchestrating Secure DevOps Life Cycles with AccuKnox



Key Takeaway

Our tooling blends CI/CD pipelines, automates policy recommendations, and conducts container vulnerability screening, ensuring a secure DevOps journey with GitOps, robust identity verification, and runtime security solutions.

AccuKnox DevSecOps – IaC



nyrahul commented on Jun 13 • edited

Author

Network Behavior Summary

Binds

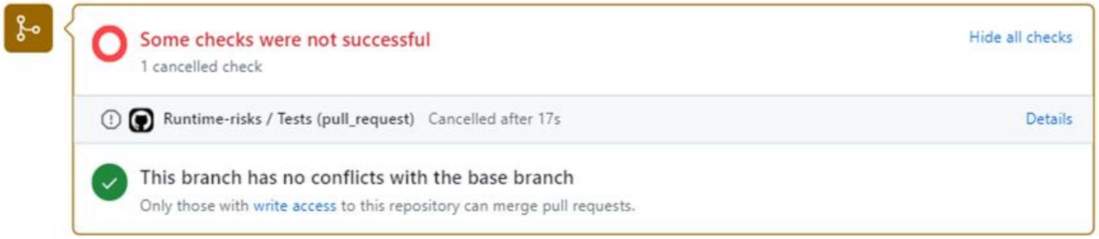
Status	PROTOCOL	COMMAND	BIND PORT	ADDRESS	COUNT
●	AF_INET	/home/sediment/build/verifier	8100	0.0.0.0	1
🚨	AF_INET	/home/vault/appver	8200	0.0.0.0	1
🚨	AF_NETLINK	/home/sediment/build/verifier			2

Egress Connections

▶ Egress Connections

Ingress Connections

Status	PROTOCOL	COMMAND	POD/SVC/IP	PORT	NAMESPACE	LABELS	COUNT
●	TCP	/bin/vault	127.0.0.1	8200			179
🚨	TCP	/bin/curl	svc/vmservice	8200	msdeploy	app=vmservice	10



Some checks were not successful

1 cancelled check

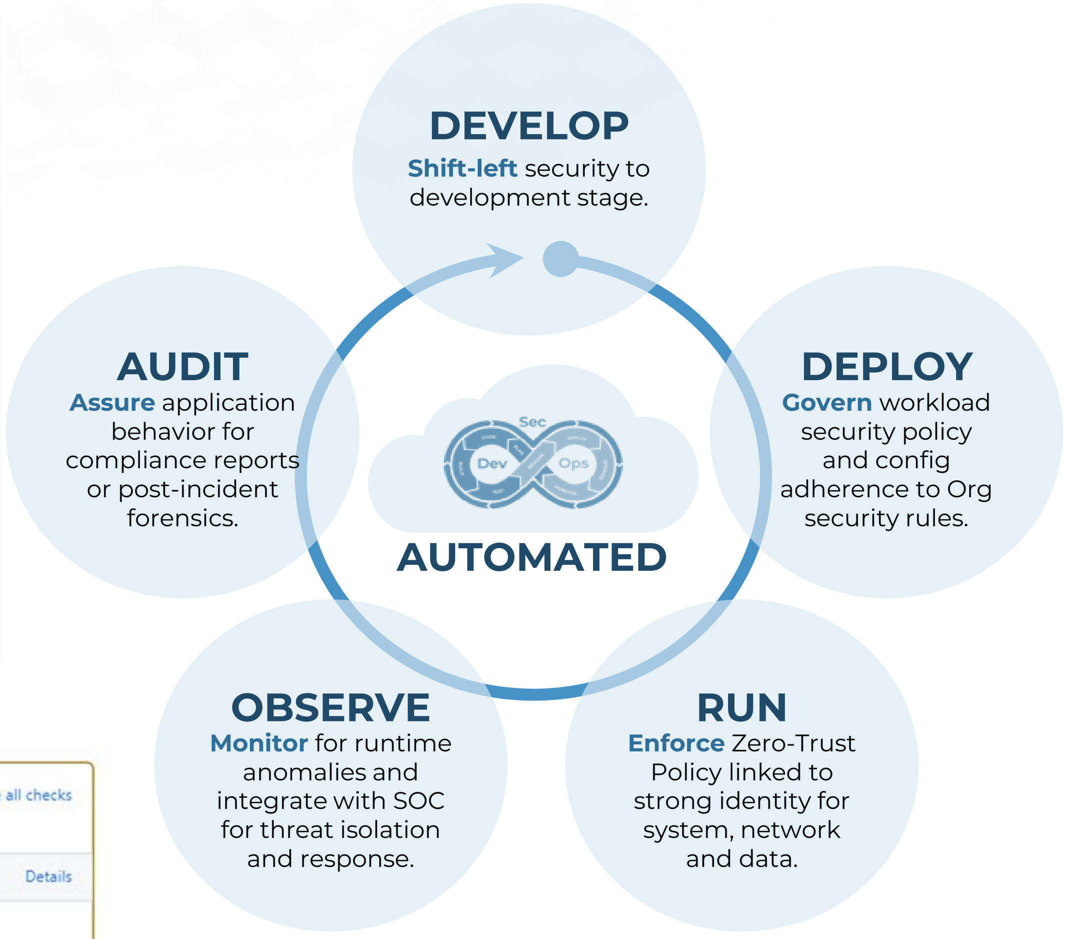
Hide all checks

Runtime-risks / Tests (pull_request) Cancelled after 17s

Details

This branch has no conflicts with the base branch

Only those with write access to this repository can merge pull requests.



DEVELOP
Shift-left security to development stage.

DEPLOY
Govern workload security policy and config adherence to Org security rules.

RUN
Enforce Zero-Trust Policy linked to strong identity for system, network and data.

OBSERVE
Monitor for runtime anomalies and integrate with SOC for threat isolation and response.

AUDIT
Assure application behavior for compliance reports or post-incident forensics.

AUTOMATED

Beware

Template misconfigurations pose a significant security risk for IaC. It potentially allows skilled attackers to exploit system security or unintentionally undermine system security.

Deploy Securely Across Public and Private Clouds

We support SaaS model for public Cloud security with an option to host customer's data on S3 bucket owned by them

Modern Infrastructure

- Public Clouds
  - AWS
  - AZURE
  - GCP

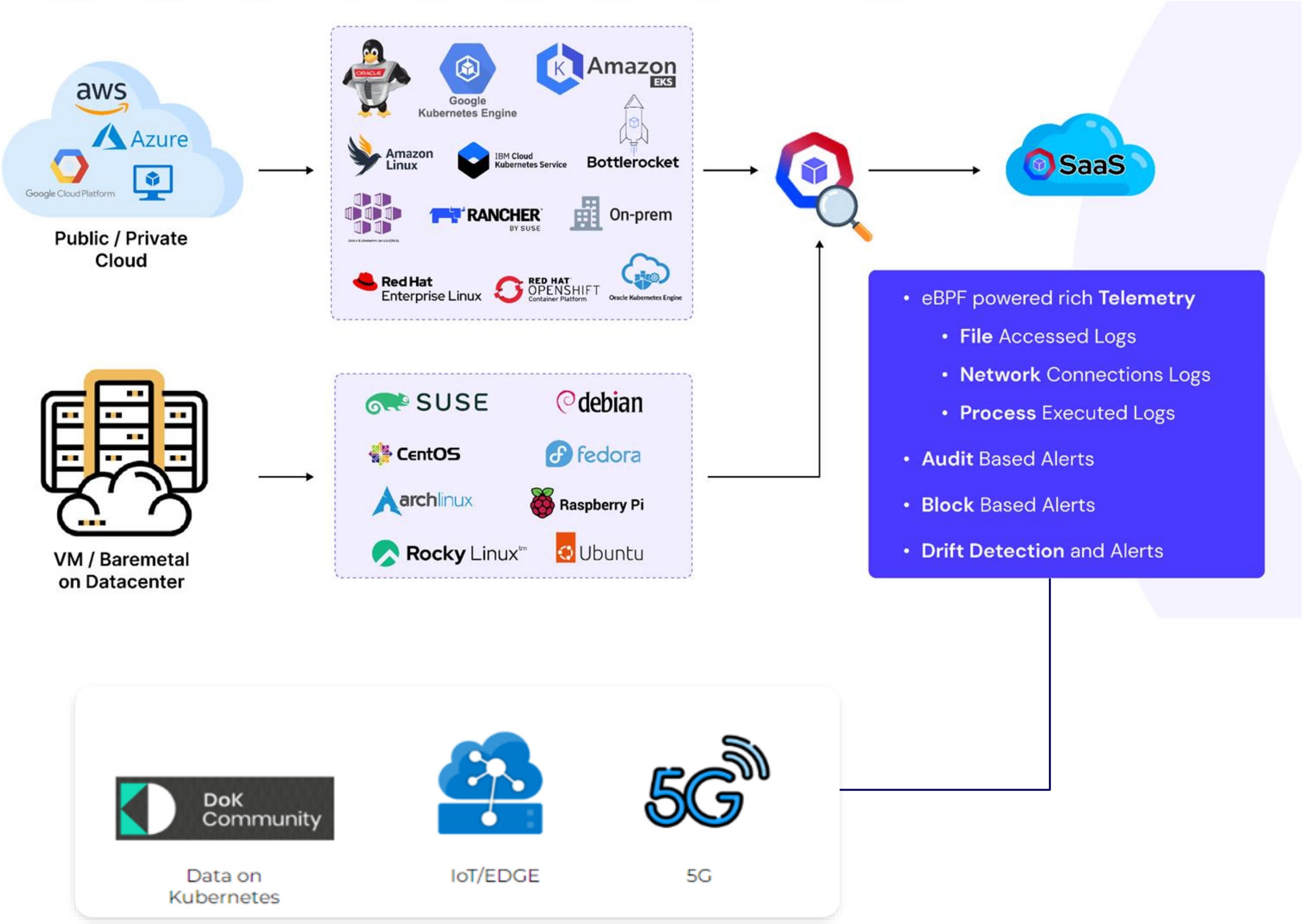
To support coverage for *Digital Transformation Journey*, we have controls and technical "know-how" to secure the following:

Modern Workload

- Kubernetes
- Containers

Traditional Workload

- VM/Baremetal



- eBPF powered rich **Telemetry**
  - **File** Accessed Logs
  - **Network** Connections Logs
  - **Process** Executed Logs
- **Audit** Based Alerts
- **Block** Based Alerts
- **Drift Detection** and Alerts

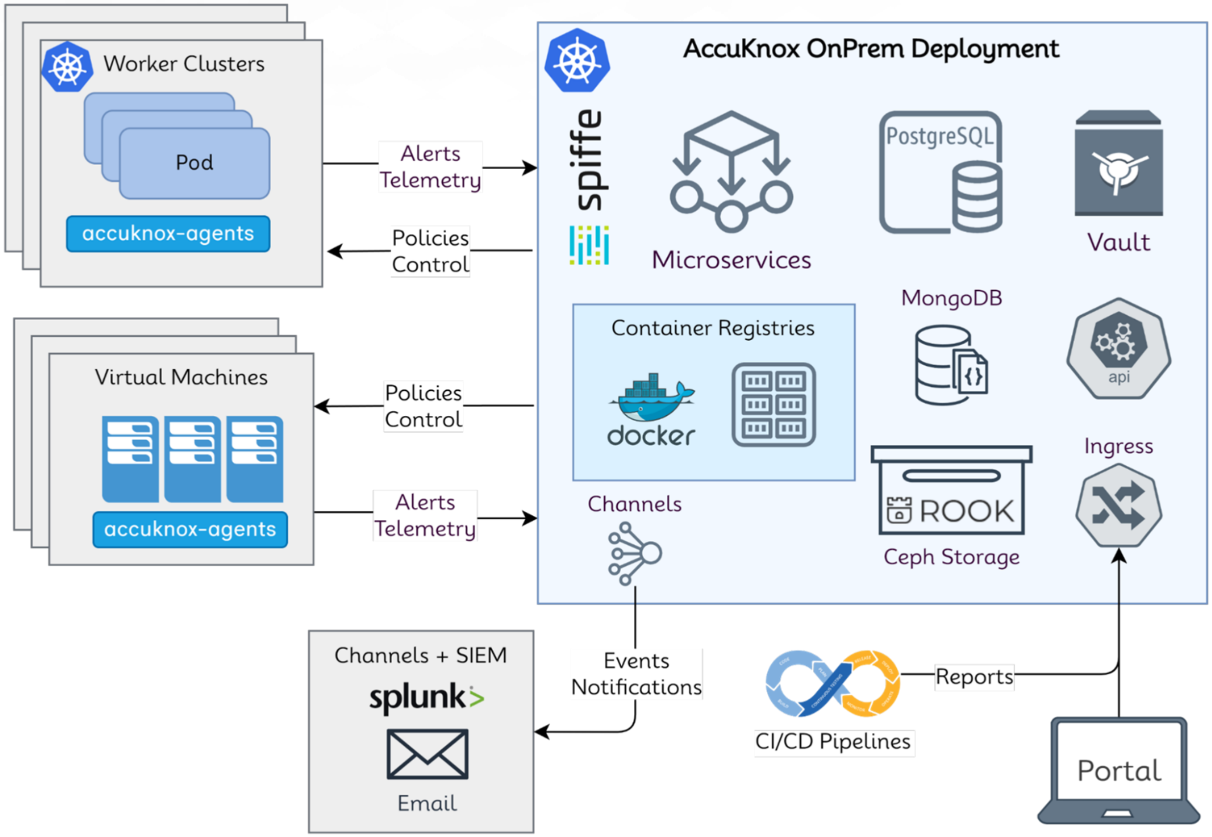
Technical Stuff

AccuKnox guarantees efficiency in public and private cloud deployments with end-to-end visibility and support for cloud-native resources and workloads across major platforms (AWS, Azure, and Google Cloud).

Air Gapped Environments

We support On-Prem air-gapped deployment model to secure infrastructure and applications on restricted environments such as

We primarily require installation of Microservices, databases, secrets management, scaling, accuknox-agents. For more info, visit [Help Documentation]



Key Takeaway

AccuKnox uses strong governance, multi-tenancy, RBAC controls, duty separation, thorough risk assessment, automation, and compliance standards to provide a safe, legal, and auditable cloud infrastructure.

Revolutionizing Security Posture with AI Insights
Automate the mundane, Empower the expert

Proactive action on drift or anomalies.

Security Posture should be easier to comprehend and propose Actionable insights

Know current security posture quickly.

Security should be reflecting current posture in a non-intrusive way (NLP)

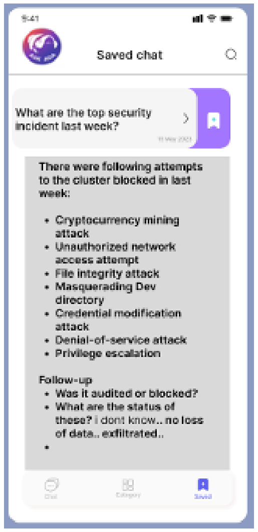
Empower different personas towards Security.

Security should provide Assistive Remediation to every security personas

Translating customized request into security configuration.

Generating automatic configuration based on simple text

CISOs, CIOs



What are the top security incident last week?

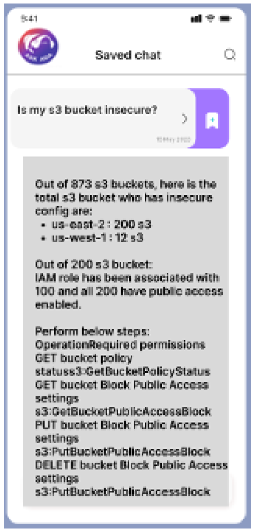
There were following attempts to the cluster blocked in last week:

- Cryptocurrency mining attack
- Unauthorized network access attempt
- File integrity attack
- Masquerading Dev directory
- Credential modification attack
- Denial-of-service attack
- Privilege escalation

Follow-up

- Was it audited or blocked?
- What are the status of these? I dont know.. no loss of data.. exfiltrated..
-

DevSecOps



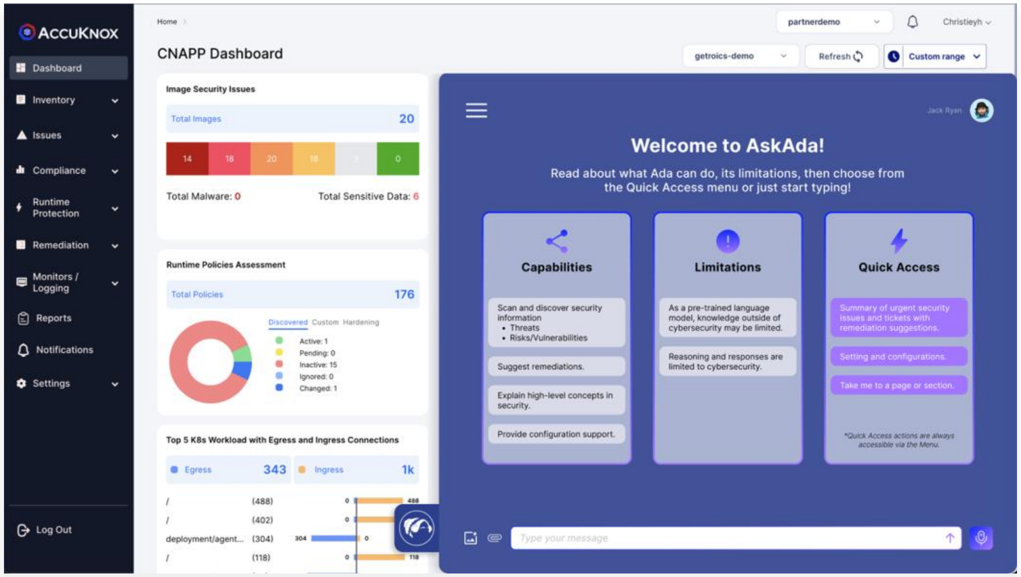
Is my s3 bucket insecure?

Out of 873 s3 buckets, here is the total s3 bucket who has insecure config are:

- us-east-2 : 200 s3
- us-west-1 : 12 s3

Out of 200 s3 bucket:
IAM role has been associated with 100 and all 200 have public access enabled.

Perform below steps:
OperationRequired permissions
GET bucket policy statuss3:GetBucketPolicyStatus
GET bucket Block Public Access settings
s3:GetBucketPublicAccessBlock
PUT bucket Block Public Access settings
s3:PutBucketPublicAccessBlock
DELETE bucket Block Public Access settings
s3:PutBucketPublicAccessBlock



Welcome to AskAda!

Read about what Ada can do, its limitations, then choose from the Quick Access menu or just start typing!

Capabilities

- Scan and discover security information
  - Threats
  - Risks/Vulnerabilities
- Suggest remediations.
- Explain high-level concepts in security.
- Provide configuration support.

Limitations

- As a pre-trained language model, knowledge outside of cybersecurity may be limited.
- Reasoning and responses are limited to cybersecurity.

Quick Access

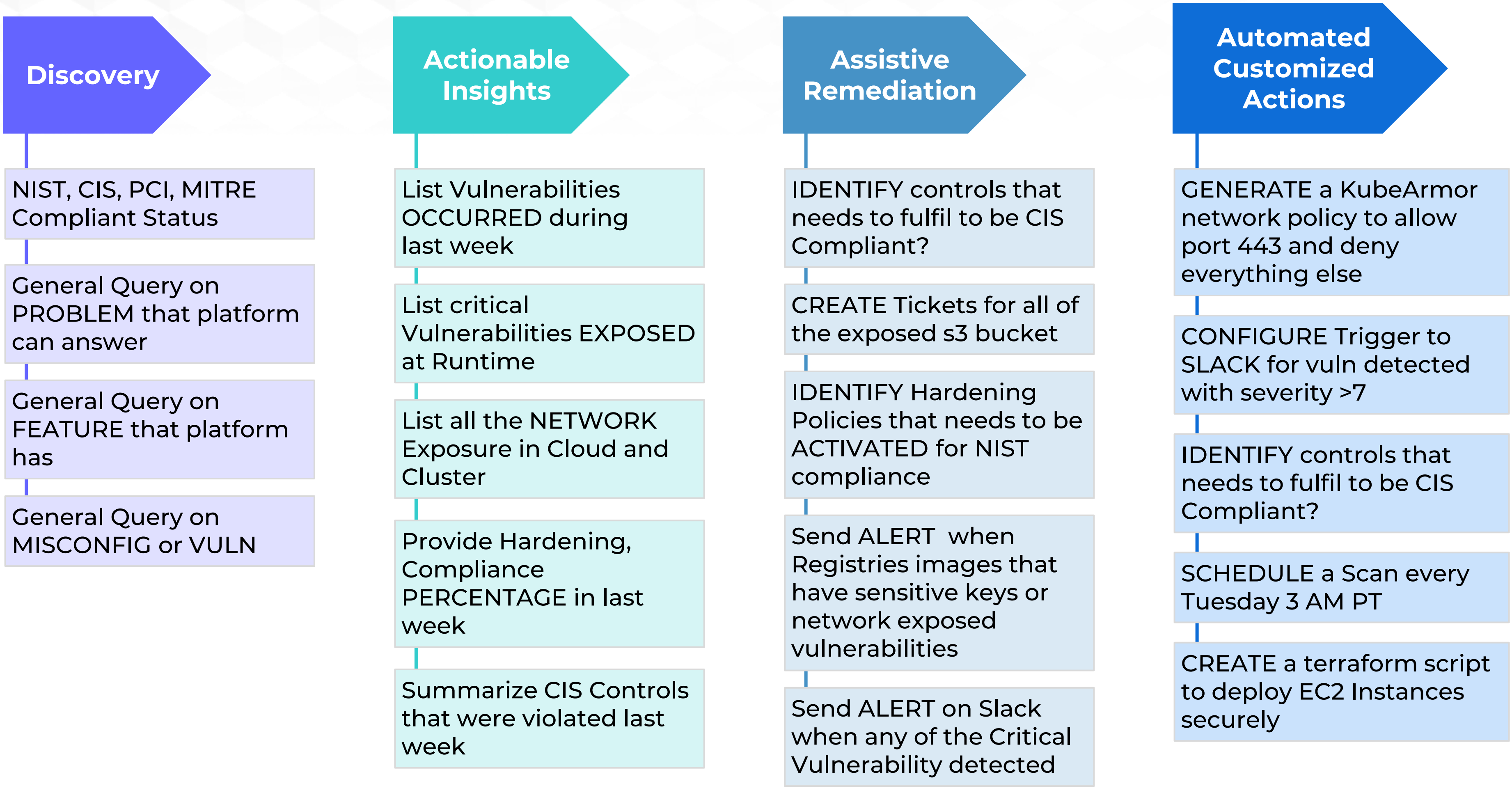
- Summary of urgent security issues and tickets with remediation suggestions.
- Setting and configurations.
- Take me to a page or section.

*Quick Access actions are always accessible via the Menu.

Key Takeaway

CyberAiDE (Ask-Ada) is a revolutionary security tool that offers proactive anomaly response, NLP-driven posture insights, and automatic configuration generation, empowering diverse security personas with actionable insights.

Streamlining Cloud Security with LLM
Automate the Mundane, Empower the Expert



Discovery

- NIST, CIS, PCI, MITRE Compliant Status
- General Query on PROBLEM that platform can answer
- General Query on FEATURE that platform has
- General Query on MISCONFIG or VULN

Actionable Insights

- List Vulnerabilities OCCURRED during last week
- List critical Vulnerabilities EXPOSED at Runtime
- List all the NETWORK Exposure in Cloud and Cluster
- Provide Hardening, Compliance PERCENTAGE in last week
- Summarize CIS Controls that were violated last week

Assistive Remediation

- IDENTIFY controls that needs to fulfil to be CIS Compliant?
- CREATE Tickets for all of the exposed s3 bucket
- IDENTIFY Hardening Policies that needs to be ACTIVATED for NIST compliance
- Send ALERT when Registries images that have sensitive keys or network exposed vulnerabilities
- Send ALERT on Slack when any of the Critical Vulnerability detected

Automated Customized Actions

- GENERATE a KubeArmor network policy to allow port 443 and deny everything else
- CONFIGURE Trigger to SLACK for vuln detected with severity >7
- IDENTIFY controls that needs to fulfil to be CIS Compliant?
- SCHEDULE a Scan every Tuesday 3 AM PT
- CREATE a terraform script to deploy EC2 Instances securely

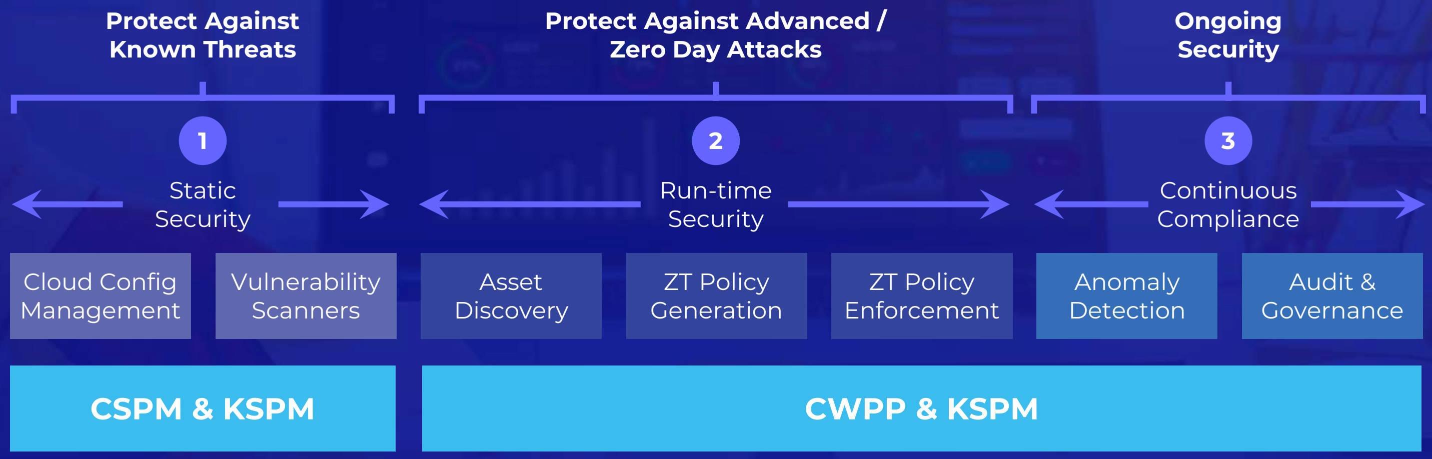
Key Takeaway

AccuKnox's CyberAiDE (Ask-Ada) is an LLM powered Cloud Security Solution that aims to
Automate the Mundane
Empower the Expert

ZERO-TRUST CNAPP

(Cloud Native Application Protection Platform]

Cloud Security at Scale with Runtime Protection



Protect Against Known Threats

1 Static Security

Cloud Config Management

Vulnerability Scanners

CSPM & KSPM

Protect Against Advanced / Zero Day Attacks

2 Run-time Security

Asset Discovery

ZT Policy Generation

ZT Policy Enforcement

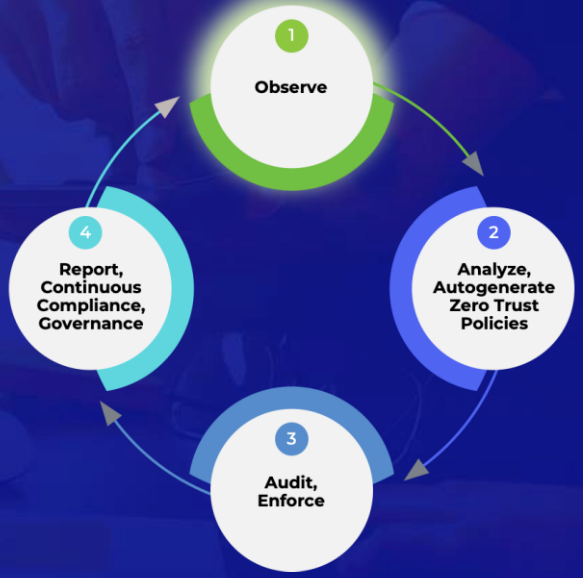
Ongoing Security

3 Continuous Compliance

Anomaly Detection

Audit & Governance

CWPP & KSPM



1 Observe

2 Analyze, Autogenerate Zero Trust Policies

3 Audit, Enforce

4 Report, Continuous Compliance, Governance

Key Takeaway

Zero Trust is a journey not a destination. As they say it is hard to get to Zero Trust, it is even harder to stay there. AccuKnox CNAPP platform allows you to get to Zero Trust in a systematic way.

CHAPTER 3

About AccuKnox

- Deep Tech, Innovation Roots
- Customer Accolades
- Innovation Patents
- Analyst praise
- Power of partnerships
- Differentiation
- Resources

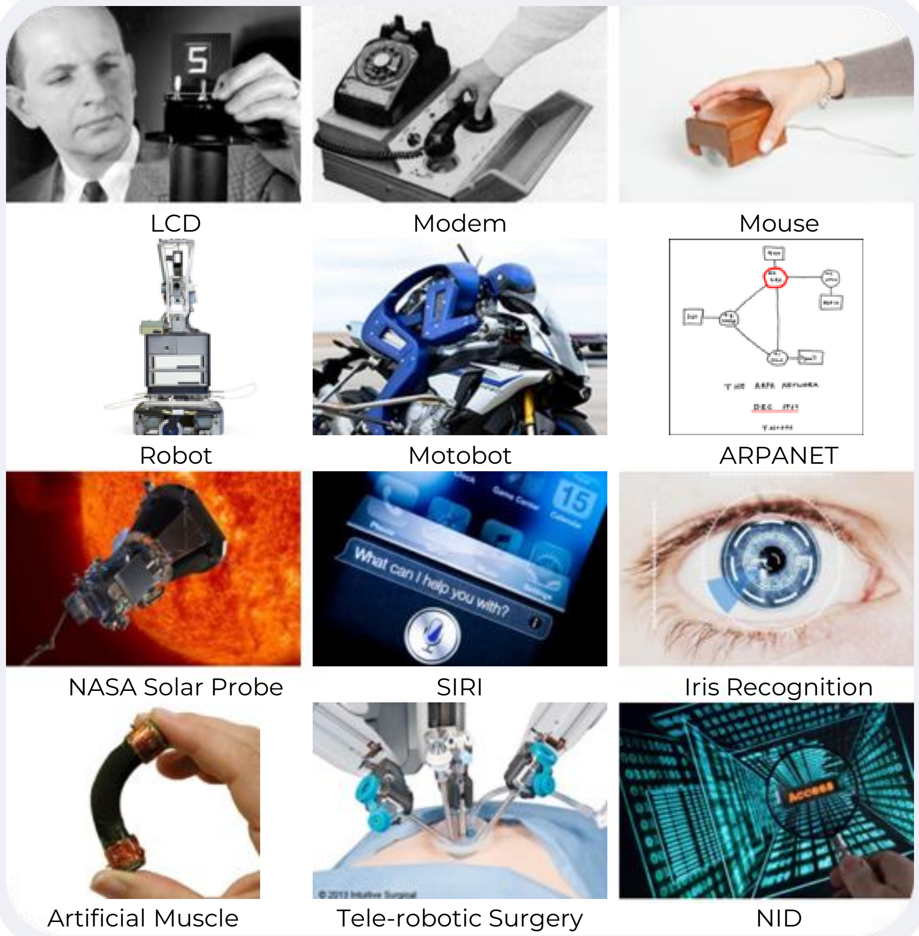
Deep Tech, Innovation Roots

AccuKnox was co-created in partnership with Stanford Research Institute

(SRI International) CyberSecurity Computer Science Labs

SRI is an investor and R&D Partner

75 YEARS OF INNOVATION SRI International



LCD

Modem

Mouse

Robot

Motobot

ARPANET

NASA Solar Probe

SIRI

Iris Recognition

Artificial Muscle

Tele-robotic Surgery

NID

Key Takeaway

SRI International, founded in 1946, has been a pioneer in creating innovative products like the mouse, modem, MICR ink, SIRI voice recognition, and robotic surgery. In the field of cybersecurity, SRI has developed anomaly detection, intrusion prevention, and intrusion detection. The company is also an R&D partner and investor in AccuKnox, contributing to the advancements in modern living.

Customer testimonials

Large US Government Contractor

"We performed an extensive analysis of comparable industry offerings and selected AccuKnox due to its support for public and private cloud and highly differentiated capabilities in the areas of Risk Prioritization, Drift Detection, and Advanced Compliance. Furthermore, we were very impressed with AccuKnox's integration with leading Vulnerability Management platforms like Nessus."

LIVANTA™

Large Cyber Insurance Provider

"Their comprehensive and integrated offering; flexible deployment options; ongoing R&D commitment; Open Source foundations; and their track record of successful partnerships made them a clear winner."

ONDA Cyber resilience, simplified.

Large Digital Health Provider

"Zero Trust security is a Clint Health imperative and commitment we have to our customers. AccuKnox's leading product combined with their successful track record of partnering with their customers forms the foundation for this objective."

clint™ The Clinical Intelligence Platform

European Cyber Service Provider

"AccuKnox's powerful combination of CSPM and CWPP; OpenSource foundations; In-line Zero Trust Security; Support for Public and Private Clouds; made them the ideal partner for us. Our client, a Large European CyberSecurity agency, was looking for a Zero Trust Security Solution that supports Private Cloud platforms. Our win is a clear testament to the value our clients see in this partnership. We look forward to many more successes ahead."

IXEL-INTERNATIONAL

Key Takeaway

Because of its sophisticated skills in Risk Prioritization, Drift Detection, and Compliance, AccuKnox is a reliable option for a wide range of sectors. It provides comprehensive, adaptable, Zero Trust security solutions and is recognized by government contractors, cybersecurity vendors, and innovators in digital health. Get a free demo here!

Pioneering Security Solutions with Patents

10+ Patents

Patented Deep Learning Algorithm for Ultra-scale Container Forensics and Stability Assessment.

Patented Federated peer-based container anomaly detection using variational auto-encoders

Patented Live eBPF Lightweight Provenance-based Data Flow tracking across Dynamic Topology Container Clusters

Patented Container Function Virtualization: high-performance L7 protocol analysis

Patented eBPF-based container-aware live sensitive data flow tracking, policy specification, and enforcement

Patented System and method for predefined policy specification for containerized workloads

Patented MUD (Manufacturer User Description) based Policy Controls for containerized workloads

Patented Sensitive Data Flow tracking in container-based environments using unified forensic streams

Patented Sensitive data flow tracking in container-based environments using trusted brokered transaction-based Provenance Graphs

Focus

With more than ten patents to its name, AccuKnox is a proud innovator in the fields of deep learning for ultra-scale container forensics, federated peer-based anomaly detection, and live eBPF-based data flow tracing across dynamic container clusters. **Get a free demo** of our state-of-the-art products on the AWS Marketplace right now.

Security Experts Laud AccuKnox Innovations

"Zero Trust run-time Cloud Security has become an organizational imperative for Companies and Governments. Accuknox' highly differentiated approach, their eBPF foundations and their seminal innovations developed in partnership with Stanford Research Institute (SRI) positions them very well to deliver a highly efficient Zero Trust Cloud Security platform."

FRANK DICKSON
VICE PRESIDENT
SECURITY AND TRUST, IDC

"Run-time Cloud Security is extremely important to detect Zero Day attacks, Bitcoin Miners, DDOS attacks, etc. Accuknox delivers a critical component of the CWPP (Cloud Workload Protection Platform). Their ability to deliver Network, Application and Data Security makes Accuknox a unique and differentiated offering."

CHRIS DEPUY
TECHNOLOGY ANALYST
650 GROUP ANALYST

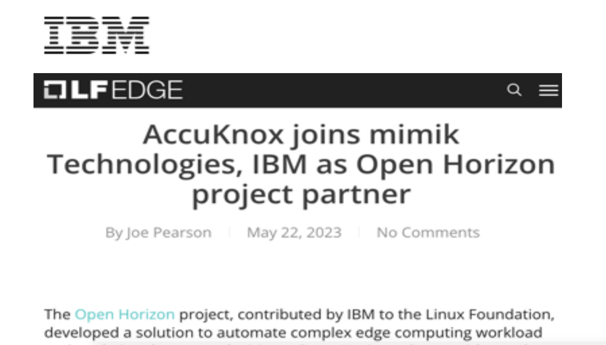
"Accuknox' foundational capabilities are innovative in the areas specific to Kubernetes security. By combining technologies like un-supervised Machine Learning and Data Provenance, Accuknox is positioned to deliver a comprehensive and robust cloud native Zero-Trust security platform to their customers."

CHASE CUNNINGHAM
RENOWNED CYBER
SECURITY ANALYST AND
ZERO-TRUST EXPERT

Key Takeaway

AccuKnox, a pioneer in cloud-native security, is renowned for its innovative Zero Trust runtime security, Cloud Workload Protection, and Kubernetes-specific capabilities, backed by a groundbreaking partnership with Stanford Research Institute.

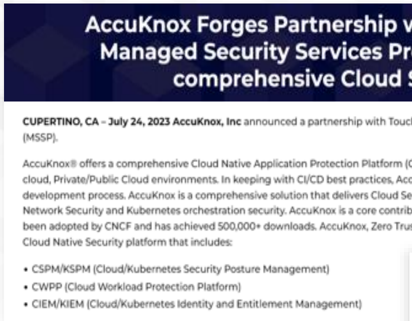
Power of Partnerships



AccuKnox joins mimik Technologies, IBM as Open Horizon project partner

By Joe Pearson | May 22, 2023 | No Comments

The Open Horizon project, contributed by IBM to the Linux Foundation, developed a solution to automate complex edge computing workload and ana
end sec
As a res
Open H

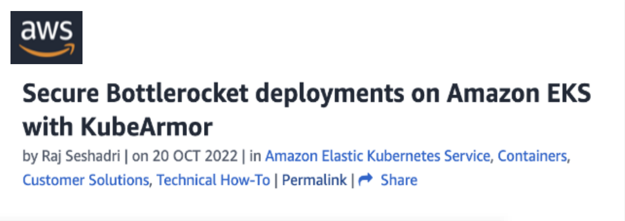


AccuKnox Forges Partnership with Touchstone Security, Managed Security Services Provider (MSSP) to deliver comprehensive Cloud Security Services

CUPERTINO, CA – July 24, 2023 AccuKnox, Inc announced a partnership with Touchstone Security, a seasoned Managed Security Services Provider (MSSP).

AccuKnox® offers a comprehensive Cloud Native Application Protection Platform (CNAPP) solution. AccuKnox delivers Zero Trust Security for Multi-cloud, Private/Public Cloud environments. In keeping with CI/CD best practices, AccuKnox focuses on finding vulnerabilities earlier in the software development process. AccuKnox is a comprehensive solution that delivers Cloud Security, Code Scanning, Container Security, API security, Host Security, Network Security and Kubernetes orchestration security. AccuKnox is a core contributor to Kubernetes run-time security solution KubeArmor which has been adopted by CNCF and has achieved 500,000+ downloads. AccuKnox, Zero Trust Enterprise CNAPP is anchored on KubeArmor and is an integrated Cloud Native Security platform that includes:

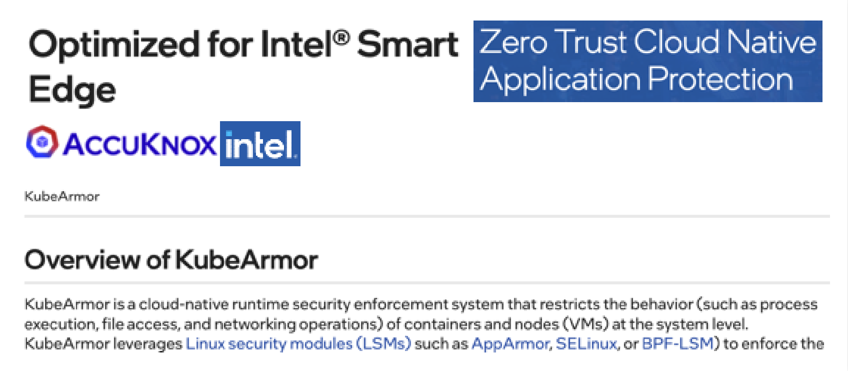
- CSPM/KSPM (Cloud/Kubernetes Security Posture Management)
- CWPP (Cloud Workload Protection Platform)
- CIEM/KIEM (Cloud/Kubernetes Identity and Entitlement Management)



Secure Bottlerocket deployments on Amazon EKS with KubeArmor

by Raj Seshadri | on 20 OCT 2022 | in Amazon Elastic Kubernetes Service, Containers, Customer Solutions, Technical How-To | Permalink | Share

es out-of-the-
useful, the



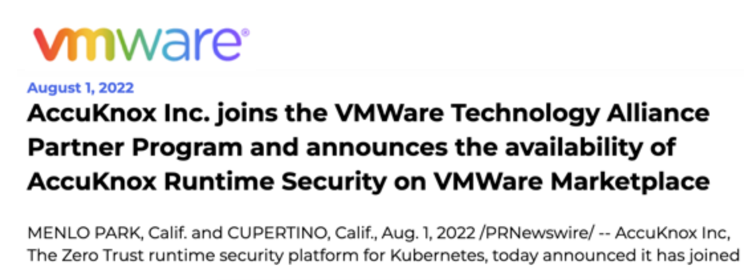
Optimized for Intel® Smart Edge

Zero Trust Cloud Native Application Protection

KubeArmor

Overview of KubeArmor

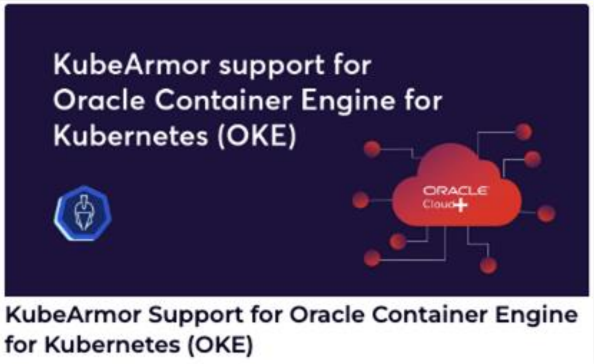
KubeArmor is a cloud-native runtime security enforcement system that restricts the behavior (such as process execution, file access, and networking operations) of containers and nodes (VMs) at the system level. KubeArmor leverages Linux security modules (LSMs) such as AppArmor, SELinux, or BPF-LSM) to enforce the



August 1, 2022

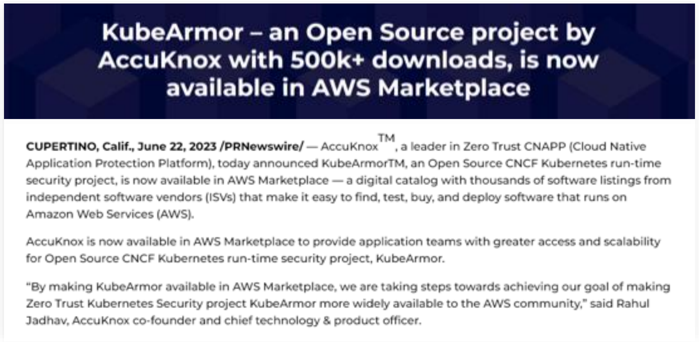
AccuKnox Inc. joins the VMWare Technology Alliance Partner Program and announces the availability of AccuKnox Runtime Security on VMWare Marketplace

MENLO PARK, Calif. and CUPERTINO, Calif., Aug. 1, 2022 /PRNewswire/ -- AccuKnox Inc, The Zero Trust runtime security platform for Kubernetes, today announced it has joined



KubeArmor support for Oracle Container Engine for Kubernetes (OKE)
ORACLE Cloud+

KubeArmor Support for Oracle Container Engine for Kubernetes (OKE)

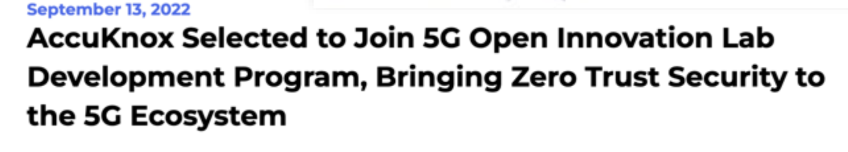


KubeArmor – an Open Source project by AccuKnox with 500k+ downloads, is now available in AWS Marketplace

CUPERTINO, Calif., June 22, 2023 /PRNewswire/ — AccuKnox TM, a leader in Zero Trust CNAPP (Cloud Native Application Protection Platform), today announced KubeArmorTM, an Open Source CNCF Kubernetes run-time security project, is now available in AWS Marketplace — a digital catalog with thousands of software listings from independent software vendors (ISVs) that make it easy to find, test, buy, and deploy software that runs on Amazon Web Services (AWS).

AccuKnox is now available in AWS Marketplace to provide application teams with greater access and scalability for Open Source CNCF Kubernetes run-time security project, KubeArmor.

"By making KubeArmor available in AWS Marketplace, we are taking steps towards achieving our goal of making Zero Trust Kubernetes Security project KubeArmor more widely available to the AWS community," said Rahul Jadhav, AccuKnox co-founder and chief technology & product officer.



September 13, 2022

AccuKnox Selected to Join 5G Open Innovation Lab Development Program, Bringing Zero Trust Security to the 5G Ecosystem

Newsflash

AccuKnox, brings together a range of industry partnerships (Software Vendors, Hyperscalers, Systems Integrators, MSSP, Resellers, etc.) to deliver customers with the most optimal solution, quick implementation approach and best ROI (Return on Investment)

Differentiation – Our Unique Offerings

#	Features	Brand A	Brand B	Brand C	Brand D	AccuKnox
1	Comprehensive CNAPP Coverage	✓	X	✓	X	✓✓✓
2	CNCF OpenSource Led	X	X	X	✓✓✓	✓✓
3	Continuous Detection and Response	✓	✓	✓	✓	✓
4	Continuous Detection and In-line Mitigation	✓✓	X	X	X	✓✓✓
5	Support for on-premises air-gapped env.	✓	X	!	X	✓✓✓
6	ASPM	✓	X	X	X	✓✓✓
7	Drift Detection and Custom Baseline	✓	X	X	✓	✓✓✓
8	Auto-Discovery of App Behavior	✓	X	X	✓	✓✓✓
9	Network Micro-segmentation	✓	X	X	✓	✓✓✓
10	Network Topology and Continuous Monitoring	✓	✓	X	✓	✓✓✓
11	Container exec and drift prevention	X	X	X	X	✓✓✓
12	5G, Edge and IoT Security	✓	X	X	X	✓✓✓

Summary

Zero Trust is an imperative in current times.

ZT is a journey not a destination.

ZT requires a comprehensive CNAPP solution.

AccuKnox is your partner in your ZT journey.

ACCUKNOX

About AccuKnox

AccuKnox provides a Zero Trust Cloud Native Application Security (CNAPP) platform. AccuKnox is built in partnership with SRI (Stanford Research Institute) and is anchored on seminal inventions in the areas of: Container Security, Anomaly Detection and Data Provenance. AccuKnox can be deployed in Public and Private Cloud environments.

www.accuknox.com   contact@accuknox.com